Delitos Informáticos

En la actualidad, las redes de comunicación electrónica y los sistemas de información forman parte de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal.

Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes. Esta tendencia implica, sin duda, numerosas y evidentes ventajas, pero va acompañada también de un riesgo inquietante de ataques malintencionados contra los sistemas de información.

En esta unidad de Delitos Informáticos desglosamos los temas:

- Concepto típico y atípico.
- Principales características.
- Clasificación.
- Tipos de ataques contra los sistemas de información.
- Pornografía infantil en internet.
- Otras clasificaciones.
- Naturaleza del riesgo.

Dichos ataques pueden adoptar formas muy distintas, incluido el acceso ilegal, la difusión de programas perjudiciales y ataques por denegación de servicio. Es posible lanzar estos ataques desde cualquier lugar hacia el resto del mundo y en cualquier momento. En el futuro podrían producirse nuevas formas de ataques inesperados.

Los ataques contra los sistemas de información constituyen una amenaza para la creación de una sociedad de la información más segura y de un espacio de libertad, seguridad y justicia, por lo que es importante abordar la temática con la mayor seriedad posible.

CONCEPTO TÍPICO Y ATÍPICO.

Dar un concepto acerca de delitos informáticos no es labor fácil, ya que su denominación alude a una situación muy especial porque para hablar de "delitos" en el sentido de acciones típicas (o tipificadas), es decir, contempladas en textos jurídico-penales, se requiere que la expresión #delitosinformáticos esté consignada en los códigos penales, lo cual en algunos países no ha sido objeto de tipificación. Empero, debido a la urgente necesidad de esto emplearemos dicha alusión, aunque, para efectos de una conceptuación, se debe establecer la diferencia entre lo típico y lo atípico.

En ese orden de ideas, según el caso, los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico).

PRINCIPALES CARACTERÍSTICAS.

1. Son conductas criminales de cuello blanco, #whiteCollarCrimes, en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden cometerlas.
2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto está trabajando.
3. Son acciones de oportunidad porque se aprovecha una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física.
6. Son muchos los casos y pocas las denuncias, debido a la falta de regulación jurídica a nivel internacional.
7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico.

9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales.
10. Ofrecen a los menores de edad facilidades para su comisión.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica en el ámbito internacional.

Las personas que cometen dichos delitos poseen ciertas características que no presentan el denominador común de los delincuentes. Esto es, los sujetos activos tienen habilidad para manejar los sistemas informáticos y en general por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible; o son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha comprobado que los autores de los delitos informáticos son muy diversos y que diferencia entre ellos es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

Al respecto, según un estudio publicado en el *Manual de las Naciones Unidas para la prevención y control de delitos informáticos* (núms. 43 y 44),90% de los delitos realizados mediante la computadora los cometían empleados de la empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que 73% de las intrusiones efectuadas eran atribuibles a fuentes interiores y sólo 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos no revela delincuencia informática, mientras otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudiera tener un empleado del sector de procesamiento de datos.

A pesar de lo anterior, teniendo en cuenta las características mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Efectivamente, el conocido criminólogo señala un sinnúmero de conductas que considera "delitos de cuello blanco", aun cuando muchas de ellas no están tipificadas en los ordenamientos jurídicos COmO delitos, entre
las cuales cabe destacar las "violaciones alas leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión dc impuestos, las quiebras fraudulentas y la corrupción de altos funcionarios, entre otras".

Asimismo, este criminólogo dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no está de acuerdo con el interés protegido (como sucede en los delitos convencionales), sino según el sujeto activo que los comete. Algunas de las características comunes de ambos delitos son las siguientes: el sujeto activo del delito es una persona de cierto estatus socioeconómico y su comisión no puede explicarse por pobreza, ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima se hallen sujetos a leyes nacionales diferentes.

Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

CLASIFICACIÓN.

Como instrumento o medio.

En esta categoría se encuentran aquellas conductas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etcétera).
2. Variación de los activos y pasivos en la situación contable de las empresas.
3. Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etcétera).
4. "Robo" de tiempo de computadora.
5. Lectura, sustracción o copiado de información confidencial.
6. Modificación de datos tanto en la entrada como en la salida.
7. Aprovechamiento indebido o violación de un código para penetrar a un sistema con instrucciones inapropiadas (esto se conoce en el medio como método del caballo de Troya).
8. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como técnica de salami.
9. Uso no autorizado de programas de cómputo.

10. Inclusión de instrucciones que provocan "interrupciones" en la lógica interna de los programas, a fin de obtener beneficios.
11. Alteración en el funcionamiento de los sistemas.
12. Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.
13. Acceso a áreas informatizadas en forma no autorizada.
14. Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo.

En esta categoría se encuadran las conductas dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos son los siguientes:

1. Programación de instrucciones que producen un bloqueo total al sistema.
2. Destrucción de programas por cualquier método.
3. Daño a la memoria.
4. Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etcétera).
5. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados,
6. Secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje, pago de rescate, etcétera).

TIPOS DE ATAQUES CONTRA LOS SISTEMAS DE INFORMACIÓN.

La expresión #sistemDInformación se utiliza deliberadamente aquí en su sentido más amplio, debido a la convergencia entre las redes de comunicación electrónica y los distintos sistemas que conectan. A efectos de la presente propuesta, los sistemas de información abarcan las computadoras personales autónomas, las agendas electrónicas personales, los teléfonos celulares, los intranets, los extranets y, naturalmente, las redes, servidores y otras infraestructuras de internet.

En su comunicación *Seguridad de las redes y de la información: propuesta para un enfoque político europeo*, la Comisión de las Comunidades Europeas propuso la siguiente descripción de las amenazas contra los sistemas informáticos:

a) Acceso no autorizado a sistemas de información.
Esto incluye el concepto de "piratería informática", la cual consiste en tener acceso de manera no autorizada a una computadora o a una red de computadoras. Puede

tomar distintas formas, que van desde el mero uso de informaciones internas hasta ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado.

b) Perturbación de los sistemas de información.
Existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos por internet es el ataque de tipo #denegaciónDeServicio (DdS), el cual es en cierta medida análogo a inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios internet (PSI) con mensajes generados de manera automática. Otros tipos de ataques pueden consistir en perturbar los servidores que hacen funcionar el sistema de nombres de dominio (DNS) y los ataques contra los "encaminadores", Los ataques destinados a perturbar los sistemas han sido perjudiciales para algunos sitios #web prestigiosos como los portales. Según estudios, estos ataques causan daños estimados en varios centenares de millones de dólares, sin contar el perjuicio no cuantificable en términos de reputación. Las empresas cuentan cada vez más con un sitio web propio y las que dependen de él para el suministro "justo a tiempo" son especialmente vulnerables.

c) Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.
El tipo más conocido de programa informático malintencionado es el virus. Los virus "I Lave You", "Melissa" y "Kournikova" son ejemplos recientemente conocidos. Existen otros tipos de programas informáticos perjudiciales. Algunos dañan la computadora, mientras que otros utilizan la pe para atacar otros elementos de la red. Varios programas (llamados "bombas lógicas") pueden permanecer inactivos hasta que se desencadenan por algún motivo (por ejemplo, una fecha determinada) y causan graves daños al modificar o destruir datos. Otros programas parecen benignos, pero cuando se lanzan desencadenan un ataque perjudicial (por eso se denominan "caballos de Troya"). Otros programas (llamados "gusanos") no infectan otros más (como los virus), pero crean réplicas de ellos y éstas generan a su vez nuevas réplicas. De este modo termina por inundarse el sistema.

d) Intercepción de las comunicaeiones.
La intercepción malintencionada de comunicaciones afecta los requisitos de confidencialidad e integridad de los usuarios y se denomina a menudo #sniffing (intromisión).

e) Declaraciones falsas.

Los sistemas de información ofrecen nuevas posibilidades de declaraciones falsas y de fraude. Usurpar la identidad de otra persona en internet y utilizarla con fines malintencionados se llama #spoofing (modificación de los datos).

Clasificación de acuerdo con las Naciones Unidas.

Por su parte, el *Manual de las Naciones Unidas para la prevención y control de delitos informáticos* señala que cuando el problema aparece en el ámbito internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de delito transnacional y su combate requiere una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera los problemas relacionados con la cooperación internacional en el área de los delitos informáticos:

1. Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
2. Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
3. Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
4. No armonización entre las diferentes leyes procesales nacionales referentes a la investigación de los delitos informáticos.
5. Carácter transnacional de múltiples delitos cometidos mediante el uso de computadoras.
6. Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Los tipos de delitos informáticos reconocidos por las naciones unidas son:

1. Fraudes cometidos mediante manipulación de computadoras.

Manipulación de los datos de entrada. Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
Manipulación de programas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado

Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de los datos de salida.
Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.
Manipulación informática aprovechando retenciones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

2. Falsificaciones informáticas.

Como objeto.
Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos.
Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

3. Daños o modificaciones de programas o datos computarizados.

Sabotaje informático.
Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:
Virus.
Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.
Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o cronológica.
Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4. Acceso no autorizado a servicios y sistemas informáticos

Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.
Reproducción no autorizada de programas informáticos de protección legal. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

PORNOGRAFÍA INFANTIL EN INTERNET.

La palabra #pornografía se deriva de pornógrafo Y se define como el carácter obsceno de obras literarias o artísticas, A su vez, el concepto de obscenidad está referido a lo impúdico u ofensivo al pudor.

Debido a que el carácter de lo que es obsceno se vincula con las variantes culturales que existen en el mundo, el concepto de pornografía infantil difiere también conforme a las prácticas de comportamiento sexual, las creencias religiosas y los valores morales que tiene cada sociedad.

Dicha situación motiva que tanto la definición como las medidas que establecen los distintos países en sus legislaciones para evitar la pornografía infantil tengan alcances diferentes.

En el ámbito internacional, la Convención sobre los Derechos del Niño adoptada por Naciones Unidas en 1989 establece una referencia a la pornografía infantil, al mencionarla como forma de explotación y abuso sexual, contra la que deberá protegerse a los niños como compromiso de los Estados miembros.

Posteriormente, en 2000, el Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, define a la pornografía infantil como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales O simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

En el Convenio sobre Cibercriminalidad del Consejo de Europa de 2013 se da una definición más amplia que incluye el material en sistemas informáticos: "La pornografía infantil comprende todo material pornográfico que represente de manera visual: a) a un menor dedicado a un comportamiento sexualmente explícito; b) a alguien que parezca un menor dedicado a un comportamiento sexualmente explícito, y e) imágenes realistas que representen a un menor dedicado a un comportamiento sexualmente explícito."

En la legislación mexicana, el Código Penal Federal se refiere la pornografía infantil como a "los actos de exhibicionismo corporal, lascivos o sexuales con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro".

El uso masivo de internet ha propiciado un crecimiento exponencial de la pornografía infantil debido a la facilidad para dar visibilidad, publicidad y acceso a todo tipo de materiales.

Internet hace factible la consulta de páginas web con material pornográfico, pero mantiene al usuario en el anonimato. Los programas "peer to peer" hacen posible compartir el material ubicado en el disco duro de las computadoras, sin dejar rastro. El correo electrónico permite enviar fotografías o videos de una punta del mundo a la otra en cuestión de segundos, sin correr el riesgo de pasar por aduanas o controles policiales. Los chats, foros y páginas de comunidades facilitan la comunicación entre pedófilos e incluso el contacto directo con menores.

El uso más actual y novedoso es lo que se ha dado en llamar #pornografíaVirtual, que consiste en la creación de contenidos sexuales con imágenes no reales, como dibujos y animaciones de menores. Esto suscita un hondo debate y provoca problemas al perseguir la pornografía infantil legal y judicialmente porque no existen las personas ni las situaciones reproducidas; a pesar de ello, fomenta el consumo de otros materiales que sí lo hacen.

Con base en el Informe sobre Pornografía Infantil en Internet de ANESVAD, se estima que en el mundo existen más de 4 millones de sitios de internet que contienen material de sexo con menores y que cada día se crean 500 nuevos. Estas páginas reciben más de 2 000 millones de visitas anuales.

Respecto a la cantidad de material que incluyen, el mismo informe señala que la mayor base de datos de pornografía infantil, elaborada por la policía británica, cuenta con 3 millones de fotografías diferentes. A esto se suman los videos, relatos y otros modos de pornografía infantil. Aproximadamente 60% de estos sitios son de pago y cobran cuotas promedio de 40 dólares al mes.

La mayoría de los sitios con pornografía infantil se encuentran en servidores de países de la antigua Unión Soviética y en algunos de América Latina, donde la legislación es mucho más permisiva con los menores.

Otros datos de la organización ECPAT, *End Child Prostitution, Child Pomography and Trafficking of Children for Sexual Purposes* que ayudan a dimensionar el problema son los siguientes:

- En el Reino Unido, a fines de 2003, la tasa anual de arrestos se incrementó 6 500% desde 1988.
- En Estados Unidos, el programa del FBI #InnocentImages registró un incremento de 2 050% en nuevos casos relacionados con la pornografía infantil entre 1988 y 200l.
- En 2005, la Policía Federal Argentina reportó que los casos de pornografía infantil se quintuplicaron en comparación con años anteriores.
- #Protégeles, una ONG europea creada para rastrear y remover pornografía infantil de internet, recibió 28 900 denuncias e identificó 1 800 comunidades en el mundo de abusadores de niños entre 200l Y 2004.
- Un estudio del Servicio Aduanero de Estados Unidos realizado en 2001 encontró 100 000 sitios en internet relacionados con la pornografía infantil.

Esa organización efectuó en 2002 una investigación denominada #Nymphasex en la que se ofrecieron "servicios con menores" y la posibilidad de comunicarse con ellos vía correo electrónico o videochat. Entre los datos que destacan, los países que efectuaron mayor número de accesos fueron Estados Unidos con 41.96%, España con 37.34% y México con 5.34 por ciento.

Convenciones internacionales.

En el ámbito internacional existen diversas convenciones internacionales que se refieren a los derechos de los niños y buscan prevenir la explotación y abuso:

- Declaración de Ginebra sobre los Derechos del Niño (1924).
- Declaración Universal de los Derechos Humanos (1948).
- Declaración de los Derechos del Niño (1959).
- Convención sobre los Derechos del Niño (1989).
- Declaración Mundial sobre la Supervivencia, la Protección y el Desarrollo del Niño (1990).
- Declaración de la Organización Mundial del Turismo sobre la Prevención del Turismo Sexual Organizado (1995).
- Declaración de Estocolmo contra la Explotación Sexual Infantil con Fines Comerciales (1996).
- Declaración y Plan de Acción de los Niños y Jóvenes Víctimas de la Explotacion Sexual (1998).
- Convenio núm. 182 de la OIT, junto con su Recomendación núm. 190, sobre la prohibición dc las peores formas de trabajo infantil y la acción inmediata para su eliminación (1999).
- Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la delincuencia organizada transnacional (2000).
- Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000).
- Convenio sobre el Delito Cibernético del Consejo de Europa (2001).
- Compromiso mundial de Yokohama (2001).
- Decisión marco 2004/68IJAI del Consejo de Europa, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil (2003).

Entre esos instrumentos destaca la Convención sobre los Derechos del Niño, que define como niño a todo ser humano menor de dieciocho años de edad, excepto cuando, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad y, que como comentamos al analizar el concepto de pornografía infantil, establece como forma de abuso sexual la explotación del niño en espectáculos o materiales pornográficos.

Otro de los instrumentos que se refiere con mayor detalle a la pornografía infantil

es el Protocolo Facultativo de la Convención de los Derechos del Niño de Naciones Unidas, que entró en vigor en enero de 2002 y que en junio de 2005 había sido ratificado por 111 países, entre ellos México.

En dicho protocolo se establece que los Estados partes prohibirán la pornografía infantil y deberán adoptar medidas en la legislación penal contra los actos de producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con fines de pornografía infantil, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente. Estas disposiciones se aplicarán también en los casos de tentativa de cometer cualquiera de estos actos y de complicidad o participación en cualquiera de ellos.

Entre otros aspectos importantes, el protocolo establece para los Estados partes lo siguiente:

- Adopción de medidas para incautar y confiscar bienes, como materiales, activos y otros medios utilizados para cometer o facilitar la comisión de los delitos, y sus utilidades.
- Adopción de medidas para cerrar, temporal o definitivamente, los locales utilizados con el fin de cometer esos delitos.
- Reconocimiento de la vulnerabilidad de los niños víctimas y adaptar los procedimientos y medidas para protegerlos.
- Protección de la intimidad e identidad de los niños víctimas.
- Adopción de medidas a fin de asegurar asistencia a las víctimas, así como su plena reintegración social y recuperación física y psicológica.
- Adopción de medidas para fortalecer la cooperación internacional para la prevención, la detección, la investigación, el enjuiciamiento y el castigo de los responsables.

Por otra parte, se consideran importantes, porque buscan acciones preventivas, el Convenio 182 de la OIT sobre la Prohibición de las Peores formas de Trabajo Infantil y la Acción Inmediata para su Eliminación, que señala que los Estados miembros deben establecer medidas inmediatas y eficaces para conseguir la prohibición y la eliminación de las peores formas de trabajo infantil, entre las que se señala el uso, el reclutamiento o la oferta de niños para la prostitución, la producción de pornografía o actuaciones pornográficas.

Por último, el instrumento internacional que detalla de manera más exhaustiva las infracciones y sanciones contra la pornografía infantil es la Decisión marco 2004/68/JAI del Consejo de Europa, del 22 de diciembre de 2003. Entre los aspectos interesantes se incluye como pornografía infantil, además del material de niños reales, el referente a una persona real que parezca ser niño y las imágenes realistas de un niño inexistente.

En esta decisión se establecen como infracciones relacionadas con la

pornografía infantil, se realicen o no mediante sistemas informáticos: producción de pornografía infantil; distribución, difusión o transmisión de pornografía infantil; ofrecimiento o suministro de pornografía infantil, y adquisición o posesión de pornografía infantil.

Regulaciones jurídicas a nivel internacional.

A finales de la década de 1970 y comienzos de la de 1980 comenzó el impulso de medidas legislativas, centradas en la prohibición de la producción, venta y distribución de la pornografía infantil.

Algunas referencias acerca de los primeros antecedentes legislativos contra la pornografía infantil son los siguientes:

En Estados Unidos los intentos por regular y proscribir la pornografía eran frecuentemente criticados como censura y violación de la Primera Enmienda. No obstante, la Suprema Corte afirmó, en un caso de 1957, que la obscenidad no estaba protegida, por lo cual podrá prohibirse el material pornográfico si cumple con la definición legal de obscenidad.

Posteriormente, en 1982 la Corte dictaminó que la pornografía infantil no estaba protegida por la Primera Enmienda, aun cuando no fuese definida de manera legal como obscena, dado que los niños no pueden consentir legalmente las relaciones sexuales.

El Congreso aprobó en 1984 el Acta de Protección Infantil, que brindaba restricciones más severas contra la pornografía infantil. En 1968 Dinamarca emitió una ley con disposiciones referentes a acciones contra la obscenidad en la palabra escrita.

En 1988 la pornografía infantil se volvió ilegal en Gran Bretaña. Otros países empezaron a legislar más recientemente: Noruega en 1992, Alemania, Francia y Canadá en 1993, Austria en 1994 y Dinamarca, España y Bélgica en 1995.

Por lo que se refiere a pornografía infantil en internet, las legislaciones difieren considerablemente de un país a otro. Algunos países no tienen referencias específicas al uso de internet, aunque se puede enjuiciar a los autores en virtud de la legislación general sobre pornografía infantil o explotación o abusos sexuales de niños, como es el caso en Haití, Portugal y Togo.

Por lo que respecta a los actos considerados ilícitos en relación con la pornografía infantil, algunos países incluyen la posesión de material (como Gran Bretaña) y otros sólo la producción, distribución y comercialización.

En Suecia, por ejemplo, está prohibido poseer pornografía infantil, pero no verla, es decir, la posesión sólo será ilegal si las imágenes o películas se descargan y guardan. La Decisión del Consejo Europeo también excluye la información pornográfica para uso privado en ciertas situaciones.

En Australia se considera el delito de "captación", que se refiere a utilizar un servicio de comunicaciones para atraer a un menor a fin de que participe en una actividad sexual.

Respecto a la edad para ser sujeto de pornografía infantil, se establece en general de menos de 18 años, pero hay países que consideran una edad menor, por ejemplo: Australia, Portugal, Polonia y Suecia. A este respecto también existen contradicciones con la edad de consentimiento para la actividad sexual, como es el caso de Suiza. En México, la Comisión del Derecho del Niño ha observado contradicción con la edad para contraer matrimonio entre niños y niñas, por posibles implicaciones.

También existen diferencias en las legislaciones en relación con las sanciones impuestas. Algunos países establecen penas máximas de 5 años y otros llegan a 10 o 12.

En cuanto a los proveedores de servicios de internet, en general se regulan por códigos propios; empero, algunos países (como Dinamarca y Suecia) consideran en su legislación responsabilidades para ellos si conservan material ilegal, después de enterarse de su existencia.

Regulaciones jurídicas a nivel nacional.

En México existen varios instrumentos jurídicos que establecen disposiciones para la protección de los niños, en general, y contra el delito de la pornografía infantil, en particular.

La reforma al artículo 4 de la Constitución Política de los Estados Unidos Mexicanos de 2000 elevó a rango constitucional el derecho de niñas y niños a satisfacer sus necesidades de alimentación, salud, educación y sano esparcimiento. Además, el deber de preservar estos derechos se amplía a los ascendientes, tutores y custodios y se especificó la obligación del Estado de proveer lo necesario para propiciar el respeto a la dignidad de la niñez y el ejercicio pleno de sus derechos.

La Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, emitida el 29 de mayo de 2000, contiene un capítulo específico para el tema de la protección en la integridad y la libertad, así como contra el maltrato y el abuso sexual.

Artículo 21. Niñas, niños y adolescentes tienen el derecho a ser protegidos contra actos u omisiones que puedan afectar su salud física o mental, su normal desarrollo o su derecho a la educación en los términos establecidos en el artículo 30 constitucional. Las normas establecerán las formas de prever y evitar estas conductas. Enunciativamente, se les protegerá cuando se vean afectados por:

A. El descuido, la negligencia, el abandono, el abuso emocional, físico y sexual.

B. La explotación, el uso de drogas y enervantes, el secuestro y la trata de personas.

C. Conflictos armados, desastres naturales, situaciones de refugio desplazamiento, y acciones de reclutamiento para que participen en conflictos armados.

En el Código Penal Federal se realizaron reformas en 2000 para tipificar los delitos de pornografía infantil y las sanciones, conforme a lo siguiente:

Artículo 201 bis 1. Si el delito de corrupción de menores o de quien no tenga capacidad para comprender el resultado del hecho o el de pornografía infantil es cometido por quien se valiese de una función pública que tuviese, se le impondrá hasta una tercera parte más de las penas a que se refieren los artículos 201 y 201 bis y destitución del empleo, cargo o comisión públicos e inhabilitación para desempeñarlo, hasta por un tiempo igual al de la pena impuesta para ejercer otro.

Artículo 201 bis 2. Si el delito es cometido con un menor de dieciséis años de edad, las penas aumentarán hasta una tercera parte más de las sanciones a que se refieren los artículos 201 y 201 bis. Si el delito se comete con menor dé doce años de edad, las penas aumentarán hasta una mitad de las sanciones a que se refieren los artículos 201 Y 201 bis de esta ley.

Artículo 201 bis 3. Al que promueva, publicite, invite, facilite o gestione por cualquier medio a persona o personas a que viaje al interior o exterior del territorio nacional y que tenga como propósito tener relaciones sexuales con menores de dieciocho años de edad se le impondrá una pena de cinco a catorce años de prisión y de cien a dos mil días multa. Las mismas penas se impondrán a quien realice las acciones a que se refiere el párrafo anterior, con el fin de que persona o

personas obtengan relaciones sexuales con menores de dieciocho años.

En abril de 2005 fueron aprobadas por la Cámara de Diputados y turnadas a la Cámara de Senadores las reformas de estos artículos, para separar en un solo capítulo los delitos de pornografía infantil. Entre los aspectos más relevantes se tipifica también el delito para quien almacene distribuya, compre e importe O exporte material, y se endurecen las penas y multas, además de hacer más específico el uso de computadoras y redes.

OTRAS CLASIFICACIONES.

Por otra parte, existen diversos tipos de delito que pueden cometerse y que se encuentran ligados directamente con acciones efectuadas contra los sistemas, como los siguientes:

1. *Acceso no autorizado*: uso ilegítimo de passwords y la entrada de un sistema informático sin autorización del propietario.
2. *Destrucción de datos*: los daños causados en la red mediante la introducción de virus, bombas lógicas, etcétera.
3. *Infracción a los derechos de autor de bases de datos*: uso no autorizado de información almacenada en una base de datos.
4. *Intercepcion de e-mail*: lectura de un mensaje electrónico ajeno.
5. *Fraudes electrónicos*: mediante compras realizadas al usar la red.
6. *Transferencias de fondos*: engaños en la realización de este tipo de transacciones.

Por otro lado, internet permite dar soporte para la comisión de otro tipo de delitos, a saber:

1. *Espionaje*: acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
2. *Terrorismo*: mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
3. *Narcotráfico*: transmisión de fórmulas para la fabricación de estupefacientes, para el lavado de dinero y para la coordinación de entregas y recogidas.
4. *Otros delitos*: las mismas ventajas que encuentran en la internet los narcotraficantes pueden ser aprovechadas para planificar otros delitos, como tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

NATURALEZA DEL RIESGO.

Existe una necesidad clara de recoger informaciones confiables sobre la amplitud y la naturaleza de los ataques contra los sistemas de información.

Los ataques más graves contra los sistemas de información se dirigen a los operadores de redes de comunicaciones electrónicas y a los servidores de servicios o a las sociedades de comercio electrónico. Los ámbitos más tradicionales pueden también verse afectados seriamente debido al nivel de interconexión cada vez mayor en las comunicaciones modernas: las industrias manufactureras, los servicios, los hospitales, los organismos del sector público y los gobiernos. No obstante, no sólo las víctimas de los ataques son organizaciones, sino también los ataques pueden causar graves daños directos y perjudiciales a los particulares. La carga económica que suponen algunos de estos ataques a los organismos públicos, a las empresas y a las personas privadas es considerable y amenaza con hacer los sistemas de información más costosos y menos asequibles a los usuarios.

Los ataques descritos los efectúan a menudo individuos que actúan por cuenta propia, a veces menores que no están del todo conscientes de la gravedad de sus actos. A pesar de ello,el nivel de sofisticación y las ambiciones de los ataques podrían agravarse.

Existe una preocupación creciente de que bandas de delincuentes organizadas utilicen las redes de comunicación para lanzar ataques contra los sistemas de información. Los grupos de piratas informáticos especializados en la piratería y la degradación de sitios internet son cada vez más activos a escala mundial, e incluso algunos intentan extorsionar a sus víctimas al proponerles una asistencia especializada tras el pirateo de sus sistemas de información. La detención de importantes grupos de "piratas informáticos o hackers" hace pensar que la piratería podría constituir cada vez más un fenómeno organizado de delincuencia.

Recientemente se han producido ataques sofisticados y organizados contra los derechos de propiedad intelectual y tentativas de robo de sumas importantes a servicios bancarios.

Las violaciones en la seguridad de las bases de datos mercantiles del comercio electrónico en las que se tiene acceso a información sobre los clientes, incluidos números de tarjeta de crédito, son también una causa de preocupación. Estos ataques suponen cada vez más medios para el fraude en el pago y obligan a la banca a cancelar y expedir de nuevo miles de tarjetas. Otra consecuencia es el daño no cuantificable a la reputación mercantil y a la confianza del consumidor en el comercio electrónico. Medidas preventivas, como requisitos mínimos de seguridad para negociantes en línea que aceptan tarjetas de pago, se analizan

conforme al plan de acción para prevenir el fraude y la falsificación de los medios de pago no monetarios.

En realidad, en los últimos tiempos; las tensiones a escala internacional han supuesto un recrudecimiento de los ataques contra los sistemas de información y, de manera concreta, contra sitios internet. Unos ataques más graves podrían no solamente tener serias consecuencias financieras, sino además, en algunos casos, implicar la pérdida de vidas humanas (sistemas hospitalarios y sistemas de control del tráfico aéreo, por ejemplo).

La importancia que le atribuyen los Estados miembros se refleja en la prioridad concedida a las distintas iniciativas de protección de infraestructuras vitales. Por ejemplo, el programa comunitario sobre tecnología de la sociedad de la información (TSI) estableció, en conexión con el Ministerio Estadounidense de Asuntos Exteriores, un grupo de trabajo conjunto Unión Europea/Estados Unidos de América relacionado con la protección de las infraestructuras vitales.

REFERENCIAS:

- Comisión de las Comunidades Europeas, Bruselas. 19/04/2000, COM (2002) 173 final. 200210086 (CNS).
- Comunicación de la Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de Regiones, Seguridad de las redes y de la informaciÓn: Propuesta para un enfoque político europeo, 6 de junio de 2001. COM (2000) 298 final.