Principales aspectos de la ciberdelincuencia

Por Pedro Molina Portela

I. Problemática [arriba]

El correo electrónico desde hace ya muchos años se ha convertido en un instrumento de comunicación independiente del tiempo y de la distancia. Los adelantos en la tecnología de las comunicaciones han posibilitado la aparición de nuevas oportunidades para la comisión de delitos sumamente complejos, en particular con relación a la ciberdelincuencia.

La inexistencia de fronteras reales es una de las características intrínsecas de internet, la cual ofrece innumerables ventajas y, como no podía ser de otro modo, inconvenientes para la persecución de actividades delictivas[1]. Es por ello que el cibercrimen (junto al terrorismo)está en vías de convertirse en una de las mayores amenazas para la seguridad mundial[2].

El fraude en línea, la difusión de pornografía infantil, los ataques piratas son sólo ejemplos de delitos relacionados con la informática que se cometen a gran escala todos los días[3]. Los daños financieros causados por el ciberdelitoson enormes[4][5]. Sólo en 2003 el software fraudulento causó daños de hasta 17.000 millones de dólares. Según algunas estimaciones los ingresos por los ciberdelitos fueron superiores a los 100.000 millones de dólares en 2007, superando las ganancias obtenidas por el tráfico de drogas en ese mismo año[6]. Igualmente, no se sabe con seguridad en qué medida las víctimas informan sobre los delitos cibernéticos. Aunque las autoridades que combaten estos delitos alientan a las víctimas a que notifiquen los casos, se teme que, en particular en el sector financiero, las víctimas (por ejemplo, los bancos) no informen los casos por miedo a que la publicidad negativa dañe su reputación. Si una empresa anuncia que su servidor ha sido objeto de actos de piratería informática, los clientes pueden perder confianza, y el costo y las consecuencias totales para la empresa podrían ser aún mayores que las pérdidas causadas por el ataque informático; además, las víctimas pueden no tener confianza en que los organismos de represión sean capaces de identificar a los delincuentes informáticos, máxime si se tiene en consideración que las estadísticas realizadas por Sarbjit NAHAL —DirectorGerente y Jefe de Inversión Temática del Bank of AmericaMerril Lynch—, informaron que el 70% de los ataques informáticos no logran ser detectados[7]. Sin embargo, si los delitos no son denunciados y los delincuentes no son enjuiciados, éstos probablemente volverán a delinquir[8]; la falta de respuestas a los delitos cometidos hace que los delincuentes piensen que el mundo cibernético es un lugar para cometer delitos impunemente[9].

A pesar de las mejoras tecnológicas y de las intensas investigaciones realizadas, el grado en que la tecnología de la información se utiliza para fines ilegales aumenta año tras año dado el reto que supone para los Estados el número de usuarios, el modo de acceso a internet, la indeterminación del ámbito geográfico, las múltiples jurisdicciones, la ausencia de una autoridad central de control, el poco tiempo para llevar a cabo las investigaciones, problemas procesales y tecnología de encriptado, entre muchos otros.

El número de usuarios:la popularidad de internet y de sus servidores van en rápido aumento, existen más de mil millones de usuarios de internet alrededor de todo el

mundo. Es por ello que el continuo aumento de la población conectada a internet, hace que también aumente el número de potenciales víctimas y de cibercriminales[10].

El modo de acceso a internet: los delincuentes, normalmente, no se abonan a un servicio de internet, ya que de ese modo podrían ser identificados, y prefieren, por tanto, optar por servicios que utilizan sin necesidad de registro. Esto explica, que los delincuentes recurran al método denominado "wardriving", que consiste en localizar redes inalámbricas desde automóviles para acceder a las mismas[11].

La indeterminación del ámbito geográfico y múltiples jurisdicciones: para iniciar cualquier política criminal hay que conocer cuál va a ser el terreno de actuación. Dicho de otro modo, saber "dónde está internet"; estamos ante uno de los grandes problemas que existen, dada la dificultad de responder con exactitud a dicha pregunta. Pero además a internet se puede acceder al instante desde cualquier parte del mundo[12]. En efecto, la circunstancia de que un sujeto pueda cometer un delito contra otro situado a miles de kilómetros de distancia del primero, mientras que la información está en otro lugar diferente al de ambos, dificulta la persecución de cualquier ilícito penal y puede llegar a producir la impunidad de los sujetos activos, en el caso de que se los llegue a identificar.Nos referimos en concreto a la aplicación espacial de la ley penal. La gran libertad para cometer delitos con absoluta independencia del territorio. El problema que se suscita es el relativo a la distinta regulación del Derecho sustantivo en los diversos Estados. A la hora de abordar este asunto, la doctrina suele traer a colación un importante caso de la jurisprudencia internacional: "el caso Yahoo!". En este paradigmático caso La Liga Internacional contra el Racismo y el Antisemitismo (LICRA) y la Unión de Estudiantes Judíos en Francia (UEFJ) presentaron una demanda contra Yahoo! por permitir la venta, en su sección de subastas, de diferentes objetos nazis como medallas, banderas e incluso uniformes de militares, alegando la violación por parte del buscador de las leyes francesas que prohíben la venta y promoción de objetos racistas, siendo que la publicidad y venta de aquellos artículos constituía una ofensa contra la memoria de un país profundamente herido por las atrocidades cometidas por los nazis. El Tribunal de Gran Instancia de París condenó a la empresa Yahoo! por la venta en territorio francés de artículos de orientación nacionalista, la cual se encontraba prohibida por el art. 645.1 del Código Penal francés e impuso a la mencionada empresa la obligación de destrucción de todos los datos, el bloqueo a los usuarios franceses a la página web y la prohibición de venta de dichos artículos.

En diciembre del año 2000, Yahoo!, previendo una solicitud de ejecución de sentencia, interpuso una demanda anteun tribunal norteamericano de California, dado que la empresa Yahoo tiene su sede en el territorio de Estados Unidos, con el fin de que el mismo dictamine la imposibilidad de ejecutar dicha sentencia en Estados Unidos, toda vez que, en dicho país su venta se encuentra permitida, siempre y cuando no se realice asociada a la apología del racismo, que la sentencia dictada por Tribunal francés, "violaba la libre expresión recogida en la primera enmienda de la constitución norteamericana", y que en el mundo de internet, resulta imposible bloquear a un número determinado de usuarios de acuerdo al ámbito geográfico.

En este sentido, el juez de primera instancia estadounidense expresó que la orden del Tribunal francés podría traspasar las fronteras norteamericanas y que aunque Yahoo! tuviera la tecnología para bloquear dichos contenidos únicamente del territorio francés, aquella medida violaría el principio de libertad de expresión. Sin

perjuicio de esto, el tribunal de alzada revocó dicha resolución por entender que el juzgado interviniente en primera instancia carecía de jurisdicción para decidir si la sentencia francesa violaba, o no, la primera enmienda, porque para ello primero LICRA y UEFJ debían solicitar ante los tribunales de Estados Unidos la ejecución de la sentencia francesa.

Otro claro ejemplo, anteriormente ya citado es la investigación de un delito cibernético en Filipinas en el año 2000 donde unos delincuentes crearon un gusano informático, "Love Bug", el cual consistía en un virus que infectó millones de computadoras en todo el mundo. En este paradigmático caso, los delincuentes utilizaron Filipinas como refugio para garantizar la impunidad de sus actos, toda vez que, las investigaciones locales se vieron impedidas por el hecho que, en esa época, el desarrollo y la difusión intencionales de programas informáticos dañinos no estaba debidamente penalizada en dicho país.La cuestión de la convergencia de legislación es fundamental, puesto que casi todos los países fundamentan su régimen de recíproca asistencia judicial en el principio de la doble incriminación, según el cual un delito debe ser considerado tal en tanto en el Estado que solicita la asistencia como en el que la presta.

El poco tiempo disponible para llevar a cabo las investigaciones en esta clase de delitos. A diferencia de lo que ocurre con las drogas ilícitas, que según el medio de transporte que se utilice, pueden tardar semanas en llegar a su destino, los correos electrónicos se envían en segundos y las pruebas pueden ser eliminadas instantáneamente[13]. La posible eliminación de cualquier rastro del hecho ilícito, constituye una de las principales problemáticas para su persecución. En este sentido, el problema procesal de mayor magnitud consiste en que los delitos informáticos no dejan huella, al menos no huellas comparables con los delitos clásicos. Por ese motivo, las dificultades de detección del delito informático se acrecientan significativamente en relación con los delitos tradicionales. Por lo tanto, será necesario establecer nuevos métodos de investigación y desarrollar nuevas herramientas de cara a la persecución de esta clase de delitos[14].

La tecnología de encriptado: Otro factor que puede complicar la investigación del ciberdelito es la tecnología de encriptado, que protege la información contra el acceso por parte de personas no autorizadas, constituyendo una práctica que dificulta a los encargados de hacer cumplir la ley, la obtención de la información contenida en dichos datos.

Dependiendo de la técnica de encriptación y la magnitud de la llave utilizadas, podría tomar décadas descifrar un encriptado. Así por ejemplo, si un delincuente utiliza un soporte lógico de encriptación con una capacidad de 20 bits de encriptación, la magnitud del espacio de la llave se situaría en torno al millón de operaciones por segundo y el encriptado podría descifrarse en menos de un segundo. Con todo, si los delincuentes utilizan un encriptado de 40 bits, podrían transcurrir dos semanas antes de poder descifrarlo. Si se utiliza un encriptado que conste de 56 bits, podrían pasar 2.285 años antes de poder descifrarlo con una sola computadora. Si los delincuentes recurren a un encriptado de 128 bits, mil millones de sistemas de computadores podrían consagrar miles de millones de años de cómputo antes de poder descifrarlo. La última versión del popular soporte lógico de encriptación PGP permite realizar encriptados de 1 024 bits[15].

Por otra parte, también nos encontramos lo que se conoce como "Dark web", "web profunda" o "web invisible", que consisten en la proporción de internet, cuya dimensión se calcula que es 500 veces superior a la internet que el ciudadano

común conoce. La misma ha sido creada mediante métodos no convencionales, como lo son el utilizar códigos en vez de direcciones de internet y pseudónimos de nivel superior creados por la Armada de los Estados Unidos que dificultan el rastreo e identificación de los delincuentes. En el año 2010 se estimó que existían más de 200.000 sitios web de esta clase.La internet profunda consiste en un conjunto de sitios web y de bases de datos comunes que no pueden ser encontradas por no encontrarse indexadas, constituyen un lugar específico de internet que se distingue por el anonimato.

La "red oscura" constituye un mercado virtual al que no se obtiene acceso buscando en la Web y en el que resulta difícil para los organismos de represión identificar a los propietarios y usuarios de los sitios digitales porque ocultan su identidad con métodos muy complejos;¿qué significa esto? Cuando ingresamos a un buscador como lo puede ser Google y realizamos una "búsqueda" el buscador no recorre la totalidad de internet, sino que lo hace únicamente en su base de datos. Este mecanismo de búsqueda se denomina "Araña web".

El contenido de la "dark web" no es analizado por los motores de búsqueda de Google o buscadores que en general conocemos, ya que estas "arañas" no rastrean bases de datos y no pueden tener acceso a páginas protegidas con contraseñas o mediante mecanismos especiales que impiden que las mismas sean indexadas.

II. Breve aproximación al concepto de cibercrimen [arriba]

Resulta inútil e innecesario buscar un concepto abarcativo de cibercrimen, quienes lo hacen, en general, entienden que la computadora o cualquier otro dispositivo de almacenamiento electrónico de datos es el elemento integrante para la comisión del delito, sea como objeto del crimen o como medio para su comisión[16]. En este sentido, el Manual de la Unión Internacional de Telecomunicaciones sobre el ciberdelito, lo define como cualquier actividad delictiva en la que se utilizan como herramienta las computadoras o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva[17].

Sin embargo, a mi entender esa definición resulta incompleta, toda vez que, la definición de ciberdelincuenciano puede ceñirse a una única modalidad o tipo delictivo, sino que la misma comprende una amplia gama de tipos ilícitos que comparten un rasgo en común, la utilización de los sistemas informáticos como objeto del crimen o como medio comisivo. En este sentido, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, firmado en Budapest, Hungría, en el año 2001, realiza una clasificación de los tipos delictivos que pueden ser cometidos por este medio; estos son: 1) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, como lo son la interceptación ilícita, los ataques contra la integridad de los datos o sistemas , entre otros; 2) delitos informáticos, entre los que incluye la falsificación informática y el fraude informático; 3) delitos relacionados con contenidos ilícitos como lo pueden ser los delitos relacionados con la pornografía infantil; 4) infracciones al derecho de autor.

En efecto, delito informático al no existir como tal, no puede constituir un tipo delictivo, es decir, el uso abusivo o pervertido de lo "informático" no puede tener entidad suficiente para mutar la naturaleza de cualquier delito, cuya esencia estará siempre en el bien jurídico protegido cuya afectación pretende evitar. Por consiguiente, lo sustantivo del hecho ilícito no está determinado por la presencia,

o no, de lo “informático”, por grandes que sean las dificultades que tal aspecto representa para su represión[18].

Por lo tanto, para concluir, corresponde establecer que la delincuencia informática no se refiere a un único tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que poseen un rasgo común,la utilización de los sistemas informáticos como objeto del crimen o como medio comisivo.

III. Modalidades comisivas del cibercrimen [arriba]

Los principales delitos existentes en el ciberespacio son llevados a cabo a fin de obtener,directa o indirectamente, un beneficio de carácter patrimonial.

Entre los delitos más frecuentesnos encontramos con los ciberfraudes (por fraude se entiende la adquisición indebida de bienes ajenos por medio del engaño).En una primera aproximación podríamos decir que los ciberfraudes son aquellos donde internet se convierte en el instrumento mediante el cual el delincuente busca obtener un beneficio patrimonial derivado de un perjuicio patrimonial a su víctima.

La Convención de Budapest —sobre la que abundaré más adelante—, en su art. 8, insta a los Estados parte a que regulen en su derecho interno el fraude informático, entendiendo que aquél constituye

“…los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona”.

Las manipulaciones relacionadas con el fraude informático constituyen un delito si causan a otra persona perjuicio patrimonial directo, pérdida de la posesión de un bien, y si el autor actuó de manera deliberada para obtener de manera ilegítima un beneficio económico para sí mismo o para otra persona.La finalidad de este artículo radica en tipificar como delito toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes.

Entre los fraudes más comunes encontramos al fraude nigeriano, el cualse caracteriza por su carácter no técnico por cuanto se refiere a una intromisión basada en la interacción humana y a menudo consiste en un ardid para engañar a las personas con el fin de obviar los procedimientos normales de seguridad. En concreto consiste en el envío de un correo electrónico a la potencial víctima presentándose como funcionario, comerciante o familiar cercano de una familia adinerada de la sociedad nigeriana u de otro país que ofrecen transferir una importante suma de dinero a cambio de una pequeña comisión. Tras la promesa de transferir miles y millones de dólares o euros a la cuenta bancaria del interesado, los motivos aludidos son la imposibilidad de mantenerlo en el país por un posible embargo, encarcelamiento de sutitular, restricciones legales o administrativas vigentes en el país[19]. Luego de lograr el interés de la víctima, le solicitan que efectúe a su nombre una pequeña trasferencia bancaria para verificar los datos de

la cuenta bancaria con la que se hará la transacción y si la misma es realizada, la víctima no volverá a saber nunca más de esos estafadores.

Por otra parte, también existe el denominado fraude de subastas o “auctionfraud”. Las subastas en línea constituyen uno de los servicios más difundidos en el cibercomercio. En 2006, por ejemplo, sólo por Ebay se vendieron mercancías por un valor superior a los 20.000 millones de dólares. Quienes cometen delitos a través de estas plataformas se aprovechan de la ausencia de contacto entre los vendedores y compradores, cualquiera puede hacerse un usuario o inventar uno, sin el más mínimo control. Debido a esta dificultad de hacer una distinción entre los usuarios genuinos y los ficticios, el fraude de subasta se ha convertido en uno de los ciberdelitos más populares, cuyas dos modalidades más comunes son las de ofrecer mercancías no disponibles a la venta y exigir su pago antes de la entrega y la de el “shilling”, donde los vendedores participan de la subasta, ofertando/pujando por su propio producto, con la finalidad de obtener un mayor beneficio económico por el mismo.

Los ciberdelincuentes también han elaborado técnicas para obtener información personal de los usuarios que van desde los programas espíahasta los ataques destinados alphishing. El término phishingdescribe una serie de actos llevados a cabo para que las víctimas revelen información personal y/o secreta. Aunque hay diferentes tipos de ataques de este último tipo, elphishing a través de mensajes electrónicos consta de tres etapas importantes. En la primera, los delincuentes identifican empresas legítimas que proponen servicios en línea y mantienen una comunicación electrónica con clientes que pueden constituir su objetivo, por ejemplo, instituciones financieras. Proceden entonces a diseñar páginas web similares a las legítimas (“sitios pirata”) solicitando a las víctimas que entren normalmente en ellas. De esta forma, los delincuentes obtienen datos personales (por ejemplo, números de cuentas y contraseñas de transacciones bancarias en línea).Con objeto de guiar a los usuarios hacia sitios pirata, los delincuentes envían mensajes electrónicos similares a los de una empresa legítima que con frecuencia dan lugar a violaciones en materia de marcas. En esos mensajes piden a los destinatarios que entren en una determinada página web para actualizar datos o proceder a verificaciones de seguridad, o bien profieren amenazas (por ejemplo, cancelar la cuenta) si los usuarios no colaboran. El mensaje electrónico falso contiene generalmente un enlace que conduce a la víctima hacia el sitio pirata.

Otro mecanismo para la obtención de datos personales y fraude es posible a través de la utilización de redes informáticas maliciosas, redes robot o “botnets”, los cuales permiten el control de computadoras a distancia, por medio de una computadora central que infectó a aquéllas mediante la instalación de un software pernicioso que las convierte en “zoombies” y de este modo les permite un acceso total. Este software en general se envía adjunto a un mail o se encuentra inserto en determinadas páginas de internet que los delincuentes programan a tal fin[20]. Además los “botnets”, estas redes de computadoras, dificultan la localización del delincuente original, ya que las pistas iníciales podrían conducir sólo a un determinado miembro de las redes robot. En este sentido, a medida que los delincuentes controlan sistemas y redes informáticos de mayor potencia, aumenta el desnivel entre las capacidades de las autoridades de investigación y las de los delincuentes[21].

Los virus informáticos son programas informáticos con capacidad de causar daños a los equipos informáticos, con la especial característica de poder replicarse a sí mismo y propagarse. Estos se activan cuando se ejecuta el programa o archivo que

lo contiene y, una vez activados, es cuando se provocan los daños para los que el virus haya sido diseñado. Gracias a su característica de réplica, cuando se activa tiene la capacidad de reproducirse copiándose en discos duros, en programas, CD's, ficheros que se envían a través de la Red, etc.Para combatir esta técnica de ataque existen los sistemas antivirus que son programas específicamente diseñados para detectar, identificar y eliminar o inutilizar el virus.

Los gusanos informáticos son un tipo de software pernicioso que se reproduce de manera autónoma y que inician múltiples procesos de transferencia de datos con el objeto de dañar toda la red[22]. Estos son parecidos a los virus, con la diferencia de que aquéllos dependen de archivos portadores para poder realizar la contaminación y sin embargo éstos son capaces de modificar un sistema operativo con el objetivo de auto-ejecutarse como parte del proceso de inicialización del sistema operativo.Para conseguir la contaminación explotan las vulnerabilidades que detectan en el sistema que se quiera dañar o se valen de algún tipo de ingeniería social con el objetivo de engañar a los usuarios y poder ejecutarse.

Su principal misión es reenviarse a sí mismo, siendo esto algo bastante simple y sencillo ya que sólo tiene que insertarse, infectar el sistema y dejar que se active. Una vez instalado utilizará la libreta de direcciones y se enviará a un determinado número de sistemas, donde se volverá a repetir el mismo proceso.

Los "troyanos" son un software dañino disfrazado de software legítimo. Éstos no tienen la capacidad de replicarse a sí mismos y es por ello que son adjuntados en cualquier tipo de software por un programador o pueden contaminar a los equipos a través del engaño. Generalmente son utilizados para espiar a las personas; se instala un programa de acceso remoto que permite monitorizar lo que esa persona está haciendo en cada momento. Por ejemplo, es muy habitual la consecución de la captura de las pulsaciones del teclado, las contraseñas o la recepción de capturas de pantalla.

El "pharming", si bien es similar, es más peligroso que el "phishing", dado que resulta aún más complicada su detección porque se trata de un programa informático pirata que desvía el tráfico de Internet de un sitio web a otro de similares características y apariencia con el único objetivo de engañar al usuario y obtener de esta manera sus nombres y contraseñas de acceso. Los datos que se obtengan a través de esta técnica se registrarán en la base de datos del sitio fraudulento.

Estos ataques suelen hacerse copiando los sitios webs de la banca online y parecidos para así obtener acceso a las cuentas bancarias de los usuarios y poder robar datos identificativos o cometer estafas suplantando la identidad de los usuarios.

El "Keyloggers" también conocido como "registro de tecleo", es un programa instalado en un equipo informático que capta las secuencias de caracteres que el usuario presiona en el teclado. Lo que se busca a través de esta técnica es conseguir los datos de usuario y contraseñas para enviarlas a otro ordenador sin el conocimiento ni la autorización de quien utilice el terminal. Se puede decir que es un tipo de programa espía o spyware.Esta técnica también permite que el receptor de la información seleccione la obtención de datos que únicamente tengan que ver

con los nombres y claves de acceso, los números de cuenta, las tarjetas de crédito, etc.

Por otro lado, internet se ha convertido en un mecanismo ideal para la comisión de otros gravísimos delitos.

En este sentido,

“Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional”[23].

El uso de internet con fines terroristas es un fenómeno que se propaga con rapidez y exige una respuesta dinámica y coordinada de los Estados. El uso de Internet para promover fines terroristas va más allá de las fronteras nacionales, lo que amplifica el efecto potencial sobre las víctimas.

Pese a que en los últimos años se viene reconociendo cada vez más la amenaza que representa el uso de Internet por los terroristas, actualmente no existe ningún instrumento universal que se refiera específicamente a ese aspecto generalizado de la actividad terrorista. Además, hay pocos programas de capacitación especializada en los aspectos jurídicos y prácticos de la investigación y el enjuiciamiento de casos de terrorismo en que se haya usado Internet.

La tecnología es uno de los factores estratégicos que llevan a las organizaciones terroristas y sus partidarios a hacer un mayor uso de Internet con una gran variedad de propósitos, incluidos el reclutamiento, la financiación, la propaganda, el adiestramiento, la incitación a cometer actos de terrorismo y la difusión de información con fines terroristas[24].

Investigadores de las Fuerzas de Seguridad y expertos académicos en el terrorismo yhadista afirman que internet es una poderosa herramienta de reclutamiento. La mayoría de los grupos terroristas islamistas son muy conscientes de ese poder y realizan notorios esfuerzos para crear materiales audiovisuales susceptibles de ser cargados a la Red. Al Qaeda cuenta con su propia productora: “AS SAHAB” (las nubes). El enorme poder de difusión de internet y las dificultades para su control y restricción lo han convertido en un instrumento verdaderamente idóneo para los fines del terrorismo yihadista, concretamente en sus labores de reclutamiento y captación[25].

Al igual, de lo que sucede con el terrorismo, en materia de narcotráfico, la expansión de la venta online ha favorecido esta clase de delitos.Las organizaciones de narcotraficantes o el vendedor ocasional se sirven de las distintas formas de comunicación que existen en la Red (correos electrónicos, redes sociales, foros de opinión o mensajería instantánea) para explotar y desarrollar su mercado. Por ello, debemos entender que la venta de estupefacientes o sustancias psicotrópicas en Internet ha aumentado considerablemente en los últimos años, debido a que la red y el tráfico online ofrecen un mayor anonimato y discreción para los “ciber-traficantes”, aprovechando la comunicación y comercialización de droga por todo el mundo y su remota impunidad[26].

Por último, con relación a la trata de personas, el Protocolo para Prevenir, Reprimir y Sancionar la Trata de Personas contiene una definición convenida por

toda la comunidad internacional, por la cual se establece que: por trata de personas se entenderá la captación, el transporte, el traslado, la acogida o la recepción de personas, recurriendo a la amenaza o al uso de la fuerza u otras formas de coacción, al rapto, al fraude, al engaño, al abuso de poder o de una situación de vulnerabilidad o a la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra, con fines de explotación. Esa explotación incluirá como mínimo, la explotación de la prostitución ajena u otras formas de explotación sexual, los trabajos o servicios forzados, la esclavitud o las prácticas análogas a la esclavitud, la servidumbre o la extracción de órganos.

Este delito incluye distintas etapas, pero por cuanto interesa al presente trabajo solamente habré de referirme a la primera de ellas, la captación.

La captación es un concepto que se traduce en atracción. Es decir, atraer a una persona, llamar su atención o incluso atraerla para un propósito definido. En lo que respecta a la trata de personas tiene un significado muy similar. Presupone reclutamiento de la víctima, atraerla para controlar su voluntad para fines de explotación. La captación se ubica dentro de los verbos que definen las acciones sancionables dentro del tipo penal de trata de personas. Algunas legislaciones han cambiado este concepto por “reclutamiento” o “promoción” aunque no son sinónimos.

El reclutamiento consiste en atraer víctimas (para controlar su voluntad), el traslado o el transporte y la recepción o acogida con fines de explotación. Ahora bien, la forma de captación variará según se trate de trata dura o blanda. La trata blanda consiste en aprovechar la especial vulnerabilidad de las personas, que desde su carencia presta consentimiento en su propia explotación, en tanto que la trata dura, consiste en la búsqueda, inteligencia, secuestro, traslado, explotación, en contra de su voluntad expresa, sin que medie su voluntad. Constituye, pues, un mayor daño a la víctima por su modalidad[27].

Entonces, conforme a ello será diferente el modo de captación. Evidentemente en el caso de trata dura, la captación se produce a través del secuestro, en tanto en el caso de trata blanda, se aprovechará la vulnerabilidad de la víctima a través de su necesidad económica, y su búsqueda de salir de la situación de pobreza material y moral, con el anhelo de cambiar su suerte.

Es así que el medio más fácil y seguro de ingreso a la red de trata será a través de la respuesta a los avisos publicitarios, que se encuentran publicados, en los medios. Diarios, revistas, en la calle a través de pegatinas o por medios informáticos (por Internet, Facebook y otras redes sociales)[28].

IV. Convención de Budapest [arriba]

El convenio fue adoptado por el Comité de Ministros del Consejo de Europa en Budapest el 8 de noviembre de 2001 y entró en vigor el 1 de julio de 2004, constituyendo el único instrumento internacional jurídicamente vinculanteque otorga carácter prioritario a la elaboración de políticas penales contra la ciberdelincuencia.

La convención de Budapest es

“…necesari[a] para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos, garantizando la tipificación como delito de dichos actos…y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detención, investigación y sanción, tanto al nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable”[29].

En este sentido, el Convenio sobre cibercriminalidad se estructura en base a los tres objetivos por el mismo que persigue: 1) Armonizar los elementos de los delitos conforme al derecho penal sustantivo de cada país y las disposiciones conexas en materia de delitos informáticos; 2) Establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procedimiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico; 3) Poner en funcionamiento un régimen rápido y eficaz de cooperación internacional.

Con relación al ajuste de la normativa penal, por la convención mencionada se instó a los Estados parte a adoptar las medidas legislativas que resulten necesarias para tipificar como delito en su derecho[30] interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático[31], la interceptación ilícita por medios técnicos de datos informáticos, los ataques a la integridad de los datos informáticos[32] o de los sistemas informáticos (daños, borrados, deterioros, alteraciones de datos informáticos). Así como también los fraudes informáticos, los delitos relacionados con la pornografía infantil y los relacionados a la propiedad intelectual.

Asimismo, con relación a la asistencia mutua, plasma importantes medidas para llevar a cabo eficazmente las investigaciones o procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas de un delito en formato electrónico. Por ejemplo, por lo dispuesto en el art. 19 se regula el registro, instando a los Estados parte a adoptar las medidas legislativas necesarias, en su derecho interno, a fin de facultara sus autoridades competentes a registrar cualquier sistema informático o dispositivo de almacenamiento informático; y la confiscación, facultando a las autoridades a confiscar o a obtener copia de los datos informáticos a los que hayan accedido conforme a lo dispuesto en el registro.

Por el art. 20, faculta a los Estados parte a aplicar medidas para la obtención, en tiempo real, de datos relativos al contenido, es decir, delitos relacionados con la pornografía infantil y las infracciones de la propiedad intelectual, entre otras. Cuando el art. 20hace referencia a “en tiempo real”lo que busca es que los Estados parte obtengan o graben estos datos relativos al contenido, a fin de conservarlos. Esto significa guardar los datos protegiéndolos contra cualquier acción que pudiera causar una modificación o deterioro de su calidad o condición actual.

A fin de garantizar la conservación de datos, el convenio también obliga a los Estados parte a promulgar leyes que exijan a los proveedores de servicios de internet conservar los datos almacenados en sus servidores durante un plazo de 90 días(renovable), si así se lo solicitan los funcionarios encargados de hacer cumplir la ley en el curso de una investigación o procedimiento penal, hasta que se puedan adoptar las medidas jurídicas apropiadas para exigir la divulgación de esos datos. Este procedimiento para la conservación de los datos almacenados tiene una importancia crítica dado el carácter efímero de los datos electrónicos y el largo

tiempo que suelen llevar los procedimientos tradicionales de asistencia judicial recíproca en casos transnacionales.

Por último, en cuanto a las medidas tendientes a poner en funcionamiento un régimen rápido y eficaz de cooperación internacional, se destaca la relativa a que, en caso de urgencia, se podrán efectuar solicitudes de asistencia mutua, o realizar comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que estos medios ofrezcan niveles suficientes de seguridad y de autenticación, con confirmación oficial posterior si el Estado requerido así lo exige. Asimismo, faculta a que un Estado informe espontáneamente a otro (es decir, sin que exista demanda previa), a fin de ayudar a que la Parte destinataria pueda iniciar o concluir investigaciones o procedimientos en relación los delitos contenidos en este Convenio.

Notas [arriba]

[1] Andrés DÍAZ GÓMEZ, El delito informático, su problemática y la cooperación internacional como paradigma de solución: El Convenio de Budapest, Redur 8, 2012, págs. 169-203.
[2] BALLESTEROSCecilia, La gran amenaza de los cibercapos, Diario El País, 27 de abril de 2015.
[3]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 13.
[4]Ciberdelito se define como cualquier actividad delictiva en la que se utilizan como herramienta computadoras o redes, o éstos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad.
[5]Ver Hayden, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, pág. 3.
[6] Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 13.
[7] KARL, Thomas, "Las tristes estadísticas del cibercrimen: 70 % de los ataques no son detectados". www.welivesecurity.com, 9/9/15.
[8]Conclusiones del 12 Congreso de las Naciones Unidas sobre la prevención del delito y la justicia penal, Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético, Brasil, 2010.
[9]Manual de la Oficina de las Naciones Unidas contrala Droga y el Delito, Compendio de casos de delincuencia organizada, Naciones Unidas, Nueva York, 2012, pág. 142.
[10]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 74.
[11]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 77.
[12]DÍAZ GÓMEZAndrés, El delito informático, su problemática y la cooperación internacional como paradigma de solución: El Convenio de Budapest, Redur 8, 2012, págs. 169-203.
[13]Conclusiones del 12 Congreso de las Naciones Unidas sobre la prevención del delito y la justicia penal, "Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético", Brasil, 2010.

[14]DÍAZ GÓMEZAndrés, El delito informático, su problemática y la cooperación internacional como paradigma de solución: El Convenio de Budapest, Redur 8, 2012, págs. 169-203.
[15]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 85.
[16]Sain, Gustavo, "El fenómeno del cibercrimen en Internet y la World Wide Web: una mirada criminológica".
[17] Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009.
[18] GUTIÉRREZ FRANCÉS, Mariluz, "Reflexiones sobre la ciberdelincuencia (en torno a la ley penal en el espacio virtual)". Universidad de Salamanca, REDUR, 2005.
[19]Gustavo Raúl SAIN, "Delito y nuevas tecnologías", Editores del Puerto S.R.L., 2012, pág. 42.
[20]Gustavo Raúl SAIN, "Delito y nuevas tecnologías", Editores del Puerto S.R.L., 2012, pág. 42.
[21]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 82.
[22]Manual de la Unión Internacional de Telecomunicaciones, El Ciberdelito: Guía para los países en desarrollo, Ginebra, 2009, pág. 31.
[23]Ban Ki-moon, Secretario General de las Naciones Unidas.
[24]Manual de la Oficina de las Naciones Unidas contra la Droga y el Delito en colaboración con el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, El uso de internet con fines terroristas, Naciones Unidas, Nueva York, 2013.
[25]Nota de DELGADO Fernando, El reclutamiento del terrorismo Yidahista, Revista Actualidad de la Fundación Víctimas del Terrorismo.
[26]Artículo publicado online de GIRÓN Javier, La venta y el tráfico de drogas online, www.del itosinforma ticos.com, de fecha 19 de marzo de 2013.
[27]Manual de las Naciones Unidas, Oficina contra la Droga y el Delito, Manual para la lucha contra la trata de personas, New York, 2007.
[28]Artículo de la Dra. PALACIO DE ARATO María de los Ángeles, Avisos engañosos: Método de captación para la trata de personas. Global Freedom Network, 2013.
[29]Preámbulo del Convenio de Budapest del 23 de noviembre de 2001 sobre la Ciberdelincuencia.
[30] Es un típico de un tratado marco y no de un tratado ley, pues establece obligaciones futuras de desarrollo en la legislación interna.
[31] Se entenderá por sistema informático todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
[32] Se entenderá por datos informáticos toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.