Material Imprimible

Curso Ciberdelitos y Derecho Informático

Módulo 5

Contenidos:

- Prevención del Ciberterrorismo
- Instrumentos de cooperación internacional
- Situación en Europa y en Latinoamérica
- Extradición y entrega de delincuentes e información

Prevención del ciberterrorismo

El Ingeniero en Sistemas colombiano Jeimy Cano, expuso en el año 2014 lo siguiente: "El ciberterrorismo es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que, utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logran intimidar o presionar a un estado y sus ciudadanos."

Algunos consideran que el terrorismo cibernético está vinculado a las vulnerabilidades propias de las infraestructuras críticas de una estado, como la energía eléctrica, almacenamiento y suministro de petróleo y de gas, bancos, telecomunicaciones, producción, suministro de agua, servicios de emergencia, transporte, entre otros sistemas que hacen parte de la dinámica económica de un estado y el bienestar general de sus habitantes.

Teniendo en cuenta que no necesariamente las vulnerabilidades son paralelas a las amenazas, estas no dejan de ser debilidades que se establecen en un sistema. Para que se considere amenaza, se va a necesitar de un actor que mantenga recursos, motivaciones y deseos de explotar estas vulnerabilidades.

Por otro lado, otros autores van a considerar que los actos ciberterroristas son acciones terroristas y lo que contempla su significado tradicional, que solamente va a diferir en el hecho de que se despliegan, principalmente, en la virtualidad.

Teniendo en cuenta estos conceptos, se han establecido modelos para poder comprender al terrorismo cibernético como una parte externa del terrorismo tradicional, para el cual debemos analizar distintos elementos, que son los siguientes:

- El fin del accionar, como por ejemplo, una organización determinada o el gobierno
- El lugar donde se adelanta el accionar
- La técnica o estrategia empleada, como pueden ser el secuestro, la violencia, una bomba, entre muchos otros

- La acción que se efectúa en sí misma
- La motivación
- A dónde pertenece el o los perpetradores
- Y si los autores son varios o solo una persona

Aún no hay una única forma estipulada de entender al terrorismo cibernético. Sin embargo, en función a lo visto, podemos definirlo como el ataque intencionado y premeditado, con una motivación ideológica o política, o bien, una amenaza de este tipo de ataque, que se manifiesta contra la información, los programas de computadoras, los sistemas de información y datos, que puede conllevar a una acción violenta contra distintos objetivos de índole civil.

A partir del ataque terrorista que se llevó a cabo de manera sorpresiva el 11 de septiembre de 2001 en Estados Unidos, fueron numerosos los cambios que se empezaron a implementar jurídicamente y en numerosas áreas en materia de seguridad. Además, conllevó a realizar reflexiones profundas.

Diferentes situaciones en las que una organización, Estado o empresa va a tender a ser más vulnerable ante eventuales ataques terroristas:

- La organización es incapaz de unir las partes de información adquiridas de varios puntos de ella, para estudiarla y determinar posibles amenazas
- La empresa u organización no guarda la memoria de antecedentes de fallas y los medios establecidos para evitarlas
- La organización no realiza un incentivo adecuado a los analistas o individuos en posiciones importantes para adelantar los análisis necesarios de la información
- La empresa fracasa en el análisis de su entorno externo e interno, y se mantiene únicamente enfocada en los fines de negocio
- La organización no realiza el ejercicio que se requiere para evitar lo ya ocurrido, como una forma de repensar sus acciones del pasado e implementar un diseño idóneo de inteligencia que le confiera construir y contribuir el futuro inmediato.

Al observar nuevas amenazas, las cuales están basadas en información analizada y procesada, con fundamentos en tendencias y objetivos verificados y, a su vez, las mismas no conciernen a la estructura de valores o creencia de las autoridades, prácticamente se ignoran. Debido a esto, el cibercrimen y el ciberterrorismo se transforman en sorpresas que podrían ser predecibles, ya que continuamente nos mandan mensajes de su presencia, que asimismo son evadidos o ignorados de forma constante, inclusive manteniendo elementos para constatar su presencia.
Si se sigue sin divisar la fuente permanente de fallas en la inseguridad de la información, así como el lugar propicio para aprender de la mente del terrorista o del delincuente informático, vamos a estar expuestos a enfrentar acontecimientos que pudieron haberse prevenido y que, llegado ese momento, únicamente se pueden tratar o controlar.

Al terrorismo cibernético lo comprenden cinco variables que van a ser parte del análisis de esta amenaza emergente, la cual puede prestarse a confusión y fallas propias de los sistemas de información dejando de esta manera sin argumentos a los analistas de inteligencia y a los demás profesionales en materia de seguridad.
Como variables propias de esta modalidad delictiva nos encontramos a las siguientes:

- Ataques hacia la información
- Difusión y promoción de ideas y consignas
- Empleo de las tecnologías de la información para trabajos de coordinación de los planes terroristas
- Ataques directos a la infraestructura de tecnologías de información
- Y utilización del medio informático para el entrenamiento de sus grupos de acción

Al analizar estas variables y los vínculos entre las mismas, podemos visualizar nuevos comportamientos que nos van a permitir ver cómo los Estados, los individuos y las

organizaciones accionarán para que el terror en la web no se transforme en una amenaza latente y predecible, la cual se advirtió pero no se pudo enfrentar.

No es posible identificar de manera precisa cuanto es que el ciberterrorismo se fundamenta en los delitos informáticos o al revés. Esto es debido a que los actores mantienen una visión mucho más abarcativa para desarrollar y conquistar información y poder. Si el delincuente se focaliza en atacar un estado y los recursos informáticos y tecnológicos propios de su labor, algunos autores lo clasificarían como un acto de ciberterrorismo. A su vez, algunos pueden insinuar acciones sancionables por la facultad punitiva ante medios informáticos de alcance estatal que responden a leyes de dicha nación, lo cual conlleva a la utilización de medios cibernéticos para vulnerar los derechos de la nación y de sus habitantes en la red.

Ante este enfrentamiento de nociones, entre los delitos informáticos y el ciberterrorismo se perciben posibles consecuencias adversas sobre las personas, estados y organizaciones, como nuevas amenazas que deben ser analizadas a fondo y de forma expedita, para así poder hacer que la incertidumbre sea menor respecto a estos temas.

El terrorismo de carácter internacional es el que más utiliza los medios informáticos para la propagación de sus ideas y sus metodologías de ataques. De esta manera, incluyen nuevas maneras de agresión, puntualmente orientadas al adoctrinamiento en el odio, para su posterior capacitación, que no mantendrá recaudos en relación al uso de métodos crueles contra sus adversarios. Debido a esto, es menester que los países combatan esta amenaza con todos sus instrumentos de carácter legal que mantengan disponibles.

A razón de disminuir los riesgos y vulnerabilidades, los países adoptan las medidas que se requieran, teniendo en cuenta que estos no van a poder realizar acciones o aplicar normativas que estén por fuera de los Tratados Internacionales. Además, los países que se encuentren afectados deben accionar a partir de su Derecho Penal antes de considerar una intervención del Consejo de Seguridad, a razón de preservar la seguridad y la paz.

El doctor en derecho Vicente Pons Gamón, en un artículo de la Revista Latinoamericana de Estudios de Seguridad del año 2017 manifestó lo siguiente: "Hay que tipificar los delitos graves suficientemente para que se puedan enjuiciar y sancionar estas conductas terroristas descritas, de forma que quede debidamente reflejada la gravedad del delito. Las acciones terroristas constituyen el máximo exponente de nuevas amenazas que el terrorismo internacional plantea a las sociedades abiertas, que pretenden poner en riesgo los pilares en los que se sustenta el Estado de Derecho y el marco de convivencia de las democracias del mundo."

Ciberterrorismo y la mirada mundial

En el ámbito jurídico de carácter internacional, se acompaña al ius ad bellum de la Carta de las Naciones Unidas. Este término se utiliza en derecho para definir las razones legítimas que un país tiene para entrar en una situación bélica, y focaliza en ciertas nociones para que se desarrolle la guerra de manera "justa".

Para la Organización de las Naciones Unidas, esta clase de agresiones cibernéticas de un país hacia otro es considerada como "uso de la fuerza", y pueden conllevar a un conflicto armado de carácter internacional. En este supuesto, el país atacado tendría derecho a defenderse de manera legítima con un ataque armado.

De manera general, el Consejo de Seguridad estima a estos actos como de agresión y amenaza hacia la paz, por lo que intervendría, dadas las circunstancias, en función de restablecer la paz y la seguridad en el marco internacional.

En un trabajo efectuado por el Grupo de especialistas del Centro de Excelencia de la Organización del Tratado del Atlántico Norte para la Ciberdefensa de Tallín, se manifiesta que el derecho internacional actual se debe aplicar a las operaciones informáticas, así como también que los países tendrán la facultad de ejercer el derecho de la legítima defensa en estos supuestos.

Según el Informe de Norton sobre delitos informáticos del año 2012, "De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, en el cuál se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los

costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a 110.000 billones de dólares en doce meses. El mismo estudio revela que por cada segundo, 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial". A partir de lo expuesto, concluimos que la principal solución a esta modalidad terrorista es la cooperación nacional.

Con todo lo mencionado, podemos enumerar los siguientes retos que mantienen los estados y las organizaciones internacionales respecto a la materia:

- Comprometer al personal y a los recursos propicios
- Mejorar las metodologías para adquirir y compartir evidencias en el marco internacional
- Perfeccionar las técnicas para localizar e identificar a los a los infractores
- Y sancionar leyes para tipificar nuevos delitos emergentes de la esfera informática.

Instrumentos de Cooperación Internacional

Desde que surgieron los ciberataques efectuados por el crimen organizado o grupos terroristas, los estados y demás organizaciones han ido accionando de manera paulatina a razón de poder enfrentar esta amenaza de índole global. De esta manera, se han formulado sistemas y estrategias de acción, para garantizar la seguridad de sus habitantes, instituciones y empresas. Así, con el paso del tiempo, estas medidas se han ido transformando y adaptando a la legislaciones de los distintos estados y organizaciones.

Es sumamente necesario tipificar adecuadamente a los delitos que vayan surgiendo vinculados a los ataques por medios informáticos. Los Estados deberán aplicar sus normativas de delitos respecto al marco internacional, particularmente, en función a las estrategias de la Organización de los Estados Americanos sobre Seguridad Informática, y a la Resolución 55/63 de la Asamblea General de la Organización de las Naciones Unidas.

Para poder cumplir la ley adecuadamente, es necesario contar con expertos dedicados a delitos de alta tecnología disponibles las 24 horas del día, los 7 días de la semana, ante posibles emergencias. A su vez, estos equipos se deben actualizar continuamente y su entrenamiento debe ser permanente.

También es importante manifestar que se necesita buscar nivelación entre los distintos Estados siempre que sea factible, y también deben efectuarse estrategias respecto a la seguridad informática, lo cual requiere el compromiso de las autoridades y la cooperación con el sector privado. Asimismo, hay que tener en cuenta que las problemáticas que surgen en esta cuestión suelen ser muy difíciles de afrontar con los presupuestos estatales, inclusive para los países desarrollados.

Debido al carácter transnacional de la delincuencia informática, se ha llegado a generar un enfoque normativo de cooperación y armonización normativa entre los Estados con el fin de enfrentar la naturaleza de esta modalidad delictiva emergente. Uno de los instrumentos más relevante en la materia es el Convenio del Consejo de Europa sobre la Ciberdelincuencia, también conocido como Convenio de Budapest. Este tratado, desarrollado en el año 2001, es el primero que le hizo frente a los delitos informáticos. A su vez, es el convenio internacional que abarca mayor uso en el desarrollo de la legislación de combate a la delincuencia informática.

Como principales objetivos del presente tratado nombramos a los siguientes:

- La prevención de las facultades procesales del derecho penal interno para garantizar la investigación y el enjuiciamiento de dichos ilícitos, así como otros delitos efectuados por medio de sistemas informáticos o evidencias en formato electrónico
- La concordancia entre los elementos de carácter nacional de derecho penal de fondo respecto a las infracciones y las disposiciones vinculadas a los delitos informáticos
- La generación de un régimen eficaz y rápido en la cooperación internacional.

Dentro del convenio van a estar definidos varios delitos vinculados al empleo de medios informáticos, a saber, fraude informático, ataque a la integridad de datos, acceso ilícito, interceptación ilícita, ataques a la integridad del sistema, los delitos vinculados con infracciones de la propiedad intelectual, falsificación informática, abuso de los dispositivos, y los ilícitos vinculados con la pornografía infantil.

En el Convenio de Budapest se exponen cuestiones del derecho procesal, como la preservación expeditiva de los datos almacenados, la preservación expeditiva y divulgación parcial de los datos de tráfico, la orden de producción, la búsqueda y la incautación de datos informáticos, la recogida en tiempo real del tráfico de datos y la interceptación de datos de contenido.

Además, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua, es decir, que son con consentimiento o están disponibles al público, y prevé la creación de una red de 24/7 para garantizar una asistencia rápida entre las Partes Colaboradoras.

Si bien en sus inicios se desarrolló en Europa, después se adhirieron otros países no pertenecientes a este continente. El 23 de noviembre del 2001, el Convenio fue firmado por Canadá, Estados Unidos, Japón y Sudáfrica, y ya hay países de Latinoamérica incorporados al convenio, como Perú, Panamá y República Dominicana. A su vez, se han considerado nuevas adhesiones, entre las que se encuentra Argentina, México, Uruguay y Chile, entre otros.

En lo que respecta a la materia procesal, el Convenio mantiene el compromiso de cada Parte Colaboradora a adoptar las medidas legislativas que se consideren relevantes para llevar a cabo los procedimientos que faciliten los procesos penales y la investigación nacional e internacional, así como también para garantizar la instauración y aplicación de poderes y procedimientos a fin de garantizar las libertades personales y la protección de los derechos humanos.

En cuanto los procedimientos establecidos, se nombrarán cuáles y en qué parte del presente convenio se trata cada cuestión:

- En el artículo 16 se expone la conservación veloz de datos informáticos almacenados, incluyendo el tráfico de datos
- En el artículo 17, la revelación parcial rápida respecto a los datos de tráfico
- En el artículo 18, el deber de presentar la información requerida a personas y proveedores de servicios
- En el artículo 19 se expone el registro de toda clase de dispositivo o sistema de almacenamiento y la confiscación de los datos cibernéticos almacenados en los mismos
- En el artículo 20, la obtención en tiempo real de datos de tráfico
- Y en el artículo 21, la interceptación de datos relacionados al contenido de comunicaciones

Es fundamental que los ordenamientos jurídicos les brinden a las autoridades competentes el poder necesario para poder acceder a los datos sobre el uso, como así también para que mantengan la facultad de conservar las pruebas, teniendo en cuanta que los procedimientos de asistencia jurídica internacional generalmente son lentos.

El artículo 29 del convenio en cuestión hace referencia a la conservación rápida de datos informáticos almacenados. "Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:

- La autoridad que solicita dicha conservación
- el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo

- los datos informáticos almacenados que deben conservarse y su relación con el delito
- cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático
- la necesidad de la conservación
- y que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación…"

A partir de lo expuesto, denotamos el énfasis de los estados para mejorar sus habilidades para compartir datos de manera rápida con el fin de que el rastro electrónico se mantenga en vigencia. El tema es que dentro del marco internacional, habitualmente los mecanismos de cooperación tardan meses o años.

Justamente, en el artículo 30 del presente convenio se enfatiza en la revelación ágil de los datos respecto al uso. El mismo expone lo siguiente: "Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.
La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:

- La solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político
- la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales."

La postura de Argentina en el marco internacional

En la Asamblea General de las Naciones Unidas del 30 de julio de 2019 titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", la respuesta otorgada por el gobierno argentino respecto a los desafíos a los cuales se enfrentaban los países para contrarrestar el empleo de los medios informáticos y las comunicaciones con fines delictivos, fue la siguiente:

En cuanto el alcance de los instrumentos internacionales, "Argentina trabajaba activamente en las actividades del Comité del Convenio sobre la Ciberdelincuencia y recomendaba a los Estados que aún no fueran partes que evaluaran adherirse a dicho instrumento a fin de fortalecer su aplicación y la adhesión de países que no fueran miembros del Consejo de Europa. No obstante, teniendo en cuenta la naturaleza global del fenómeno de la ciberdelincuencia y la necesidad de contar con mecanismos que permitieran responder a dicho fenómeno de manera global, la Argentina apoyaba tanto los procesos en el marco del Convenio del Consejo de Europa, como aquellas instancias de discusión que buscaban avanzar, en el marco de las Naciones Unidas, hacia la negociación de un marco jurídico universal en la materia."

Sobre las dificultades para el acceso transfronterizo a las pruebas digitales, la respuesta fue que "La principal dificultad en la mayoría de los casos se presentaba debido a que los datos que constituían la prueba se encontraban alojados en una jurisdicción distinta de aquella donde el delito era juzgado y, en casi todos los casos, en poder/control de empresas privadas. Las soluciones propuestas hasta el momento a esos problemas,

como la Ley de los Estados Unidos por la que se Aclara el Uso Transfronterizo Lícito de Datos, la cual está vigente, y la iniciativa de la Unión Europea en materia de pruebas digitales, que está en trámite, no contemplaban acabadamente las necesidades de terceros países."

Acerca de la insuficiente capacidad para medir los resultados en materia de intercambio de información y buenas prácticas, la respuesta de Argentina fue que "En muchos casos resultaba difícil mensurar los resultados en materia de intercambios de buenas prácticas y de información enunciados en los acuerdos."

Respecto a las dificultades en la actualización del marco normativo en relación con el avance tecnológico, Argentina manifestó que "Mantener actualizado el marco normativo penal, tanto de fondo como procesal, conllevaba muchas dificultades, que eran más graves en los países con sistemas legales codificados."

En cuanto al bajo nivel de concientización en la población y en las organizaciones, "Un aspecto esencial de la lucha contra el delito era el referido a la prevención. En el delito cibernético, la prevención se vinculaba directamente a la concientización, de las personas y las organizaciones, acerca de los riesgos y amenazas que entrañaba el uso de las tecnologías de la información y las comunicaciones. Era necesario formular planes nacionales de concientización bajo los cuales se articularan los esfuerzos e iniciativas, tanto privadas como públicas, de un modo que permitiera dotar de coherencia a los mismos y optimizara el uso de recursos."

Sobre la responsabilidad del sector privado expone que "El sector privado desempeñaba un papel fundamental en relación con los desafíos que planteaba el delito cibernético. La responsabilidad de las empresas se verificaba en aspectos como el control y la gestión de las vulnerabilidades en materia de datos que presentaban las plataformas y los dispositivos, y el uso de las redes sociales con fines delictivos. Más allá de la

cooperación voluntaria del sector privado, era preciso analizar la necesidad de reglas de cumplimiento obligatorio."

Por último, sobre el crecimiento de los riesgos, se manifiesta que "La profusión del uso de dispositivos inteligentes de relativamente bajo costo que permitían el acceso a Internet sin un nivel mínimo de seguridad aumentaba la superficie de potenciales ataques y el alcance del delito cibernético. Para hacer frente a este crecimiento se requerían políticas de Estado y estrategias de responsabilidad corporativa complementarias. Los proyectos impulsados por algunos Estados para contar con mecanismos que les permitieran desencriptar información de dispositivos/aplicaciones o mecanismos de puerta trasera suponían un riesgo. También se habían de evaluar los instrumentos de penetración informática y extracción de información o monitoreo que proponían diversos cuerpos judiciales."

A partir de lo expuesto, vemos que la República Argentina había establecido que los desafíos fundamentales que afrontaba como país en relación a la persecución de los delitos e investigación de los mismos, efectuados a partir del uso de los medios informáticos y las comunicaciones, constaban de las siguientes cuestiones:

- La necesidad de contar con herramientas e instrumentos de informática e investigación forense propicios para el personal del poder judicial y las fuerzas de seguridad
- El requerimiento de normativas procesales que contemplen las características particulares de las evidencias digitales
- La carencia actual de definiciones y tipificaciones adecuadas en las leyes penales
- La importancia de capacitar a los funcionarios del sistema judicial penal
- El mejoramiento de los mecanismos de cooperación internacional
- Y la necesidad de mejorar la cooperación de las empresas del sector privado, particularmente de los servicios de red.

Argentina también afirmó que la capacitación en relación a la materia del delito informático y la recolección de pruebas de carácter digital era el desafío más próximo para alcanzar una persecución penal eficiente. Así, el país indica que los esfuerzos deben esta focalizados en extender los saberes de los funcionarios del sistema y así lograr que las leyes y los instrumentos internacionales vigentes sean aplicados adecuadamente. A partir de esto, no solamente se brinda una respuesta propicia contra esos delitos, sino también, el respeto por los derechos de las partes que constituyen el proceso.

Asimismo, Argentina manifestó la valoración de los aportes efectuados por las organizaciones regionales e internacionales, entre ellas, las Naciones Unidas, la Unión Europea, la Organización de los Estados Americanos, y el Consejo de Europa.

El Ministerio de Justicia de la República Argentina opera continuamente respecto a elaborar normas procesales para la adquisición de evidencia digital que sirva a la legislación provincial y federal, ya que dicho país, en su carácter federal, implica la coexistencia de un sistema de justicia federal junto a los sistemas de justicia provinciales, lo cual puede generar una mayor complejidad en cuanto a las respuestas internacionales al delito informático y evidencia digital.

A partir de esto se implementó la creación de distintas unidades fiscales especializadas, por lo que se comenzó a obrar en las distintas jurisdicciones para que adoptaran este modelo con el fin de agilizar el intercambio de información en las investigaciones.

Por último, se remarca que Argentina expuso un desafío adicional respecto a la insuficiencia de recursos financieros para llevar adelante las modificaciones requeridas, tanto en las fuerzas de seguridad como en el poder judicial, lo que conlleva a esfuerzos sostenidos manifestados como una política del gobierno.

Situación en Europa y en Latinoamérica

El continente Europeo es el más avanzado en materia de seguridad informática y el que posee la mayor cantidad de trabajos efectuados respecto a la misma. En relación a esto, se ha diseñado en el Consejo de Europa, con el fin de proteger a las sociedades de la amenazas emergentes ocasionadas a partir de delitos informáticos, la Convención sobre

el delito informático y su Protocolo sobre la xenofobia y el racismo, los programas de cooperación técnica sobre el delito informático, y el Comité de la Convención sobre el delito informático.

A partir de ellos se siguen las mismas pautas en relación a dar seguimiento y valoración a los acuerdos del comité, generar acuerdos comunes, y construir capacidades creando programas de cooperación.

En febrero del 2019 en Rumania, se llevó a cabo una Conferencia de Justicia Penal. Allí se reunieron más de 100 especialistas en justicia penal de alrededor de 40 países, dentro de los cuales estaban incluidos funcionarios públicos e individuos de la esfera privada. Esta conferencia fue organizada en conjunto a la Presidencia rumana del Consejo de la Unión Europea y el Consejo de Europa, y fue precedida por un acontecimiento en el aniversario de la Oficina del Programa de Delitos Cibernéticos del Consejo de Europa.

Con la idea de ilustrar la situación mundial, se expondrá un resumen relacionado a los temas tratados, que probablemente se irán extendiendo en el globo. Igualmente, el resumen constituye un ejemplo propicio respecto a los planteamientos sobre la complejidad y el manejo de los delitos en el ciberespacio.

En primer lugar podemos manifestar que generalmente este tipo de amenazas informáticas que mantienen las sociedades se presenta de forma similar en las distintas partes del mundo. Gran parte de los ataques provienen de otros estados o la evidencia se encuentra en el extranjero, y para poder entender estas amenazas y poder contrarrestarlas, se precisa tener un enfoque que traspase a los estados y a las regiones individuales.

En segundo lugar, las autoridades que correspondan a la justicia penal deberán tener medios propicios para resguardar las evidencias electrónicas e intentar ir a la par de la evolución del crimen cibernético y de la tecnología, debido a que, en caso contrario, la confianza en el estado de derecho puede disminuir. Es necesario de manera inmediata buscar soluciones adicionales ante la imperiosa necesidad.

En tercer lugar se puede expresar que la evidencia electrónica constituye un tema fundamental en el interés de los estados, las entidades privadas y las personas. Si bien se

hace necesaria una solución, llegar a un acuerdo que reconcilie los distintos intereses, es un desafío.

En cuarto lugar, los desafíos con respecto a la justicia penal en el medio informático incluyen, además, la necesidad de generar la asistencia legal mutua de manera más eficiente y manejar el problema de la evidencia en la web, que puede provenir desde lugares extranjeros, desconocidos o incluso múltiples. Por ende, se deben abordar los problemas vinculados a la jurisdicción y la pérdida del conocimiento respecto a la ubicación. Paralelamente, los conceptos de jurisdicción están cambiando, y cada vez se considera más relevante la ubicación de los datos de las personas en posesión o control de los estos.

Asimismo, La delincuencia en el ciberespacio constituye una amenaza transversal y, por ende, la cooperación entre las instituciones, de carácter privado, público e internacional, es fundamental. De igual manera, la cooperación en todas las escalas deberá respaldarse a partir de programas que desarrollen capacidades.

También puede decirse que es necesaria una mayor comprensión respecto a cómo concordar los requisitos en correspondencia a la protección de datos y justicia penal de manera práctica, particularmente en un contexto que trasciende las fronteras, y cómo los intereses de protección de datos se equiparan con los intereses públicos relevantes, como la seguridad pública y la prevención del delito. Los estados deberán proteger los derechos de los individuos también contra los delincuentes.

En séptimo lugar, las decisiones judiciales que se han tomado recientemente indican que el acceso a la información del suscriptor es considerado una pequeña interferencia a los derechos de los individuos, pero, asimismo, puede ser necesario efectuar un análisis caso por caso que mantenga en cuenta la circunstancia específica. Ello, además, puede aplicarse a la base legal respecto al procesamiento de datos, en donde, dependiendo de la circunstancia, se puede requerir el cumplimiento de una obligación legal, consentimiento del interesado, intereses vitales y públicos importantes o intereses legítimos del que controla los datos.

En octavo lugar, se contempla la negociación de un Protocolo Adicional respecto a la cooperación internacional de forma mejorada y con acceso a la evidencia en la “nube”

que equipare de mejor manera a las Partes de la Convención con los medios propicios para la defensa del estado de derecho en el medio informático.

Igualmente, se propone un continuo desarrollo en las habilidades respecto a delitos informáticos y evidencia electrónica, que abarcan desde el fortalecimiento de la legislación estatal, hasta la capacitación de legistas e investigadores. Se sugiere el implemento de instituciones especializadas y la cooperación a partir de las diferentes escalas, lo que constituye una parte fundamental de la respuesta y contribuye a abordar las necesidades imperiosas. La Oficina del Programa de Delitos Cibernéticos del Consejo de Europa en Bucarest, capital de Rumania, ha realizado en los últimos años más de 600 actividades que incluyen a más de 120 países. Esto evidencia que el desarrollo de capacidades opera y genera un impacto.

También es importante destacar que hasta la fecha, la Convención de Budapest sigue siendo el acuerdo internacional más importante respecto a la ciberdelincuencia y a la evidencia digital, y la cantidad de países que forman parte del mismo continúa aumentando. Las partes deberán efectuar un uso propicio de este tratado y atribuir sus enunciados en la legislación estatal, particularmente en el derecho procesal, con garantías y condiciones.

A su vez, se realizarán consultas adicionales con entidades pertenecientes al sector privado y especialistas en protección de datos para culminar disposiciones particulares respecto a la cooperación directa con los proveedores.

Otra cuestión a tener en cuenta es que el desarrollo de respuestas ante las amenazas llevadas a cabo por la Unión Europea y el Consejo de Europa seguirá reforzándose de forma mutua, complementaria y consistente.

Asimismo, las propuestas legislativas de la Unión Europea se complementan con medidas técnicas, como un portal propicio para la Unión Europea, a razón de efectuar solicitudes de evidencias digitales cuya noción está apta y que las autoridades de los países miembros de la Unión Europea están ahora motivados a probar.

Del mismo modo, el paquete de evidencia electrónica de la Unión Europea, que consta en un Reglamento respecto a una orden europea obligatorio de conservación y producción, así como una directiva complementaria respecto a los representantes

legales de los proveedores de servicios que se implantarán dentro de la Unión Europea, brindará un sistema eficaz para que los países miembros de la Unión Europea puedan acceder a las pruebas digitales con salvaguardias.

Por último, a medida que la tecnología y el panorama de amenazas cibernéticas evolucionan, las propuestas de evidencia digital de la Unión Europea y el Protocolo del Convenio de Budapest deberán prever y hacerse a prueba del futuro.

Los estados de Latinoamérica mantienen una falta de homogeneización respecto al ámbito de la normativa penal vinculada a los delitos informáticos, ya que han optado por distintas posturas en relación a las maneras de regular.

Algunos han decidido sancionar leyes especiales, donde inclusive, como es el caso de República Dominicana, incorporan nociones propias, parte penal material y procesal, principios, y hasta se han creado organismos focalizados en su investigación y persecución. Igualmente, la mayoría de los países de esta región han decidido realizar modificaciones de carácter parcial en los Códigos Penales vigentes, adaptando las figuras penales tradicionales con el objetivo de que sea factible su aplicación en los delitos informáticos.

A partir de la carencia de armonización, se visualizan diferencias en dos escalas. La primera de estas radica en las diferencias entre los estados respecto a los criterios políticos en relación a la consideración de si tal acción nociva debe ser o no sancionada como un ilícito penal.

En una segunda escala, dentro de los estados que han dado una respuesta de carácter positiva sobre la primera escala, pueden observarse discordancias respecto a los criterios penales estipulados como necesarios para la conformación del tipo penal.

Frente a esto, se comprende que existe una necesidad de mejorar las escalas de armonización y evolución legislativa en la temática, con el objetivo de aplacar la existencia de huecos legales en la región que ayuden a que se despliegue la delincuencia informática.

En cuanto a la situación del Mercosur respecto a la temática, citamos a los abogados Santiago Deluca y Enrique del Carril quienes, en el año 2017, manifestaron lo siguiente:

"En el MERCOSUR no existe un derecho penal común. No obstante, se observa una creciente corriente orientada a la adopción de normas generales de política criminal tendiente a combatir diversos actos delictivos. Ello se cristaliza en la creación de normas de cooperación internacional en materia penal, con el objeto de lograr la asimilación y adecuación 'macro' de las legislaciones penales de los Estados Parte."

Deluca y del Carril prosiguen y manifiestan que "El MERCOSUR se encuentra encaminado en la creación de un espacio integrado de cooperación en materia penal, más allá del aspecto puro y exclusivamente económico. Y, principalmente, analizar cómo se presenta hoy en día la modalidad conocida como cibercrimen y la utilidad de las herramientas señaladas para lograr combatirlo."

Podemos decir entonces que si bien no hay un proyecto de creación de un instrumento internacional semejante, se han ideado propuestas interesantes para la cooperación y coordinación respecto a las cuestiones de seguridad informática y delincuencia informática.

Recientemente el MERCOSUR destacó la relevancia de las Reuniones con las Autoridades para tratar la Privacidad y Seguridad de la Información y así poder tomar posiciones respecto a las políticas e iniciativas consensuadas en la materia de seguridad informática, la protección de los datos personales, la privacidad, la prevención, la confianza en la utilización de la web y el combate de la delincuencia por medios informáticos, a partir de estrategias y políticas que promuevan la coordinación regional, respetando las singularidades de los Estados que la conformen.

Esta reunión, llamada RAPRISIT, en la cual predominan las características técnicas sobre las jurídicas, viene realizando contribuciones relevantes para planificar estrategias de manera conjunta en la temática de seguridad informática y lucha contra la delincuencia cibernética.

Lo ideal sería que este órgano tomara el protagonismo necesario para así analizar la normativa de los Estados Parte con el fin de determinar si estas cumplen con los estándares que se desean en función a la protección de datos personales.

Extradición y entrega de delincuentes e información

Con respecto a la etiología de la palabra, extradición viene del latín "ex", que significa "afuera", y "traditio", que significa "transmisión".

Por extradición entendemos al procedimiento judicial penal-administrativo a partir del cual una persona que es condenada o acusada por un ilícito conforme a la normativa de un país es detenida en otro y devuelta al primero en cuestión para que se le realice el juicio correspondiente o para que cumpla la pena que ya se le había impuesto.

Actualmente, si bien hay una cooperación internacional bastante activa para la represión de los ilícitos, sigue existiendo la normativa de que un país tiene la obligación a conceder la extradición de un criminal extranjero únicamente si hay tratados internacionales con el país requirente o una Convención Internacional respecto a la extradición, de la que ambos países sean pertenecientes. Cuando no existe un tratado o convención internacional, el país requerido tiene la facultad para poder acordar la extradición, pero no va a estar obligado a concederla. Sin embargo, la obligación descripta no es absoluta, debido a que conforme a su legislación interna, no se cumplen los requisitos preestablecidos para dicho fin.

Por lo antedicho, la mayoría de los tratados de extradición van a requerir que el país que la pide manifieste y evidencie la existencia de una causa para castigar o enjuiciar al requerido, y que el ilícito imputado se encuentre tipificado de esa forma tanto en la legislación penal del país requirente como del país requerido.

En cuanto a los procesos de extradición de Argentina, cuando se trate de una extradición pasiva, el trámite judicial se regirá por los tratados multilaterales o bilaterales existentes entre la República Argentina y el país requirente. En caso de que no haya, el trámite se regirá según lo establecido en la Ley de Cooperación Internacional en Materia Penal número 24.767, bajo ofrecimiento de reciprocidad para casos análogos. La referida ley también se utiliza para interpretar lo dispuesto en los tratados internacionales, y para complementarlos en las situaciones que no estuvieran contempladas en estos instrumentos de cooperación internacional. En cambio, si se trata de una extradición

activa, el trámite se va a desplegar en función a los tratados que existan entre la Argentina y el estado requerido, y en caso de que no haya ninguno, se manejará según la normativa del estado referido.

A modo de dejar en claro ambos conceptos, procedemos a definir las extradiciones activas y pasivas.

La extradición activa se da cuando la Argentina pide la extradición de un individuo que se encuentra detenido en otro país por un ilícito que efectuó en la jurisdicción nacional. Ante la carencia de tratados internacionales, las condiciones y el proceder serán regulados por la normativa del estado al que se le solicita la extradición.

Por su parte, la extradición pasiva se refiere a cuando un individuo es requerido por otro estado debido a que se halla en territorio nacional, con el fin de ser sometido al proceso de enjuiciamiento o a cumplir una pena impuesta y por eso dicho país pide su entrega.

Todas las solicitudes de extradición nacen a partir de una orden de detención. No obstante, es factible requerir una detención con carácter preventivo con fines de extradición a partir de la presentación de un pedido formal de extradición, sin necesitar una solicitud previa de detención provisoria, debido a que el pedido presume, además, una exigencia de detención preventiva.

A partir de la Dirección General de Cooperación Regional se da un aviso a las Fiscalías respecto a detenciones de carácter preventivo que se presenten por la Organización Internacional de Policía Criminal. El Juez Federal competente que intervenga debe efectuar una audiencia en 24 horas, con el objetivo de informar y escuchar a la persona que se encuentre detenida para que se designe el legista defensor, entienda los motivos de su detención y la factibilidad de dar su consentimiento a ser extraditada.

En la circunstancia en la cual el requerido manifieste su voluntad de ser extraditado, la Ley de Cooperación Internacional en Materia Penal va a establecer que el Jurista de la causa está obligado a resolver dicha petición de forma inmediata. Este pedido puede surgir en cualquier parte del proceso y debe resolverse de manera inmediata. Llevado a

cabo el juicio de extradición, el Jurista va a resolver si la extradición va a ser procedente o no, y esta sentencia va a ser pasible de apelarse de manera ordinaria ante la Corte Suprema de Justicia de la Nación.

Una vez firme una decisión del Poder Judicial que declare la procedencia de un pedido de extradición, comienza la tercera etapa, denominada "decisión final", que se encuentra en cabeza del Poder Ejecutivo que, a su vez, ha delegado esa responsabilidad en el Ministerio de Relaciones Exteriores y Culto. En caso de que en sede judicial se declare improcedente el pedido, resulta una decisión definitiva y el referido Ministerio se limita a comunicarla al país requirente. En cambio, en caso de que se resuelva favorablemente, el Juzgado interviniente deberá remitir a la Cancillería el expediente judicial completo, a los fines de que resuelva de manera definitiva la concesión o no de la extradición, dentro de los diez días hábiles posteriores a su recepción, pudiendo denegarla en base a las causales establecidas en el artículo 10 de la ley 24767 de Cooperación Internacional.

Con respecto a las pruebas e informaciones entre países, nos encontramos ante el hecho de que existen potenciales problemas probatorios, que lejos de contar con los medios del convenio de Budapest, surgen inconvenientes en el rastreo de comunicaciones electrónicas a través del mundo y la recolección de pruebas digitales. Además, puede pasar que los tratados respecto a la asistencia jurídica mutua, vigentes en ese momento, no contemplen de manera propicia las pruebas digitales.

Soluciones factibles en el contexto Argentino para la recolección y el intercambio de evidencia:

- Desarrollar estándares técnicos de carácter internacional y organizarse internacionalmente para el manejo de las evidencias informáticas
- Tener en cuenta la Convención sobre los Delitos Informáticos, la cual opera como un tratado de asistencia jurídica mutua para aquellos estados que no lo mantienen. Acá, las partes del tratado van a acordar ofrecerles asistencia a los otros estados para que adquieran y brinden pruebas digitales
- Por último, la asistencia de la Organización Internacional de Policía Criminal, es decir, la INTERPOL, y demás organizaciones similares.

Hoy en día es fundamental resolver las dificultades que enfrentan las autoridades alrededor del mundo para identificar el delito informático. Asimismo, se manifiesta la necesidad imperiosa de cooperar internacionalmente para lograr actualizar las leyes argentinas a la par de la evolución tecnológica, así como las técnicas investigativas, las leyes de extradición y la asesoría judicial para lograr alcanzar a los criminales. Si bien ya se han iniciado numerosos esfuerzos al respecto, quedan muchos por hacer.