Estados Unidos de América

El Gobierno de los Estados Unidos de América se complace en responder a la invitación extendida a los Estados Miembros para presentar sus perspectivas sobre el alcance, los objetivos y la estructura (los elementos) de la nueva convención, con respecto a la aplicación de las resoluciones 74/247 y 75/282 de la Asamblea General de las Naciones Unidas. Los Estados Unidos anhelan cooperar con otros Estados Miembros de las Naciones Unidas y partes interesadas para redactar un instrumento mundial centrado en mejorar la investigación y la judicialización de la ciberdelincuencia, en forma congruente con los derechos y obligaciones vigentes y basándose en ellos. Los Estados Unidos reiteran la importancia de mantener un proceso abierto, inclusivo, transparente y multilateral que permita a todos los Estados Miembros negociar de buena fe soluciones prácticas, basadas en el consenso y bien fundamentadas que, en nuestra opinión, propiciarán la adhesión generalizada a un nuevo instrumento mundial para el combate del ciberterrorismo.

El plazo propuesto para nuestro trabajo da lugar a una cronología rigurosa incluso en circunstancias normales, pero nuestras laborales actuales se emprenderán contra el telón de fondo de una pandemia global. En consecuencia, resulta aún más esencial realizar tareas focalizadas y eficientes para negociar un instrumento mundial contra la ciberdelincuencia. Lamentablemente, mientras gran parte del mundo se ha abocado a combatir la pandemia de COVID-19, los ciberdelincuentes han explotado el cambio y la dependencia globales resultantes de las tecnologías digitales. La ciberdelincuencia es una amenaza directa a la seguridad y el bienestar de las sociedades y personas de todo el mundo. Existe cooperación de larga data para fortalecer nuestra capacidad colectiva a fin de combatir esta explotación, y podemos seguir apoyándonos en esos éxitos con consideración minuciosa de soluciones prácticas. A la luz de la

inmediatez de la amenaza de la ciberdelincuencia, resulta incluso más esencial concentrarse y actuar con resolución en las labores para negociar un instrumento mundial para el combate de la ciberdelincuencia.

Dicho instrumento contra la ciberdelincuencia se debería concentrar en afianzar la cooperación internacional y suministrar herramientas prácticas para preparar a las autoridades del orden nacionales a hacer frente a la ciberdelincuencia, del mismo modo que lo hicieron otros instrumentos de las Naciones Unidas respecto de otras formas de delitos transnacionales, como la corrupción, el narcotráfico, la trata de personas y el contrabando de migrantes. Asimismo, el instrumento debería garantizar que la autoridad nacional recabe y obtenga pruebas electrónicas pertinentes para cualquier tipo de delito, no solo los delitos habilitados por el ámbito cibernético, y promueva la cooperación internacional en tales casos. Al igual que con todos los instrumentos de las Naciones Unidas contra la delincuencia, estas herramientas deberían incluir límites y salvaguardias adecuados, en el contexto de los marcos nacionales en vigor, para abordar la privacidad y las libertades civiles, sin dejar de lado el respeto pleno por los derechos humanos. Asimismo, el instrumento para el combate de la ciberdelincuencia debería abordar la necesidad creciente de asistencia técnica y ofrecer vías para que los Estados Miembros soliciten dicha asistencia.

Al inicio del proceso de redacción por parte de los Estados Miembros es esencial reconocer que no trabajamos en un vacío. Tan importante como la definición del contenido del presente instrumento es reconocer lo que escapa a su correcto alcance. En las Naciones Unidas y en otros foros intergubernamentales y multilaterales hay tareas valiosas en curso sobre otras cuestiones cibernéticas más allá del alcance del ciberdelito. Es importante que no dupliquemos ni menoscabemos ese trabajo, tanto para evitar conflictos de obligaciones como para no restar valor

a nuestro objetivo de producir un instrumento práctico, específico para combatir la ciberdelincuencia. Un intento por abordar cada cuestión cibernética en este instrumento de justicia penal se tropieza con el riesgo de sumir a estas negociaciones en debates inespecíficos y tangenciales que escasamente contribuirían a combatir la ciberdelincuencia y sólo desacelerarían el avance hacia un instrumento útil.

En particular, los Estados Miembros no deberían ahondar en temas de gobernanza cibernética o ciberseguridad en un instrumento sobre delincuencia dedicado a combatir la ciberdelincuencia. Si bien con frecuencia se perciben como dos caras de la misma moneda, el cumplimiento de las leyes en materia de ciberdelincuencia es responsabilidad esencial del gobierno, mientras que la ciberseguridad es la responsabilidad de una gama de actores públicos y privados. El mandato del comité ad hoc (AHC) se centra en la formulación de un instrumento de justicia penal sobre asuntos delictivos para facilitar una respuesta internacional a la ciberdelincuencia, que implique definir y sancionar la conducta delictiva en el ciberespacio. El AHC no está habilitado para dictar normas globales para conducta no delictiva en línea. Incluso los conceptos de gobernanza cibernética y la ciberseguridad en un tratado sobre la ciberdelincuencia no satisfarían el objetivo de un instrumento simplificado y efectivo que atraerá el apoyo amplio de los Estados Miembros.

Conforme fue reafirmado por la Resolución 75/282 de la Asamblea General, resulta esencial que las negociaciones hacia un nuevo instrumento para el combate de la ciberdelincuencia no obstaculicen mecanismos actuales, como instrumentos multinacionales y regionales, que ya brindan una gama de herramientas para combatir en forma efectiva la

ciberdelincuencia[1]. Si nos remitimos a instrumentos en vigor que han probado ser exitosos podemos forjar un mejor consenso para este instrumento nuevo y evitar cuestiones políticas y divisivas. Deberíamos ser guiados por los logros que emanan de la aplicación de otros tratados de justicia penal de las Naciones Unidas, como la UNTOC. La UNTOC ha probado ser de suma utilidad porque el instrumento está dirigido a tipos centrales de actividad delictiva organizada, al tiempo que incluye disposiciones amplias sobre cooperación internacional que podrían aplicarse a cualquier tipo de delito grave cometido con fines de lucro por tres o más personas. En consecuencia, las Partes han recurrido a la UNTOC en forma satisfactoria millares de veces, incluso para combatir delitos, como incidentes con programas maliciosos secuestradores y la explotación de menores con fines sexuales.

Los Estados Unidos reiteran una vez más la importancia de mantener un proceso abierto, inclusivo y transparente que permita a todos los Estados Miembros y a las partes interesadas negociar de buena fe soluciones prácticas, basadas en el consenso y bien fundamentadas, que en nuestra opinión constituyen la mejor manera de propiciar la adhesión generalizada a un nuevo instrumento mundial contra el ciberterrorismo.

Penalización de los delitos de ciberdelincuencia centrales

En primer lugar y lo que es más importante, todo instrumento nuevo debería garantizar un mandato nacional para recabar y obtener pruebas electrónicas para cualquier tipo de delito. Estos mandatos son imprescindibles para que los países investiguen y judicialicen en forma eficiente prácticamente todos los tipos de delitos, dado que muy pocos delitos en la actualidad

[1] Resolución 75/282, Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Aprobada por la Asamblea General el 26 de mayo de 2021 y disponible en https://undocs.org/en/A/RES/75/282.

son realizados por completo fuera del mundo digital. El instrumento debería también permitir la cooperación internacional para compartir pruebas electrónicas de cualquier tipo de delito, sujeto a una disposición de enfoque flexible sobre la doble incriminación tal como existe en la UNTOC y la UNCAC[2]..

Además, la cooperación internacional eficiente exige que los Estados Miembros cuenten con la legislación nacional adecuada para penalizar delitos de ciberdelincuencia centrales. Una perspectiva compartida de los delitos sustantivos centrales y las autoridades procesales de respaldo entre los Estados Miembros es esencial para evitar crear refugios para los ciberdelincuentes. Los estudios realizados por la UNODC muestran que los países por lo general convergen en la conducta central que debería ser penalizada por normativa específica en materia de ciberdelincuencia, con numerosos convenios multinacionales y normas penales nacionales que contienen disposiciones comunes. De igual manera, la interpretación internacional de la doctrina procesal legal que respalda las investigaciones efectivas de la ciberdelincuencia es constante. En consecuencia, los profesionales cuentan con dos décadas de experiencia acumulada y variada en la investigación de la ciberdelincuencia que demuestra la viabilidad constante de doctrina sustantiva y procesal adoptada comúnmente para investigar la ciberdelincuencia.

Un nuevo instrumento para el combate de la ciberdelincuencia debería definir y aplicar los delitos cibernéticos, que son delitos en los que una computadora o datos son el blanco de la actividad delictiva, así como ciertos delitos que permite el entorno cibernético, es decir delitos en los que se usó una computadora para su facilitación. Esta primera categoría principal de delitos que ha de ser definida por este nuevo instrumento comprende los que no pueden ser cometidos

[2] Artículo 18 de la UNTOC, párrafo 9; Artículo 46 de la UNCAC, párrafo 9. Aunque las disposiciones de las dos convenciones difieren en cierta medida, ambas ofrecen un margen de discreción considerable a los Estados partes receptores en materia de prestar asistencia, especialmente en lo que respecta a las medidas coercitivas.

sin el uso indebido de computadoras o sistemas de red y que, por ende, no existían como delitos antes del advenimiento de los sistemas de computadoras. Los delitos cibernéticos pueden pertenecer completamente al mundo digital. Para los delitos cibernéticos centrales, como los ataques de denegación de servicio o el daño a computadoras y datos, se requiere de normas específicas para los aspectos cibernéticos porque en la mayoría de las jurisdicciones las leyes penales se interpretan de forma rigurosa y las leyes tradicionales que abordan conceptos conocidos, como invasión y vandalismo, suelen ser inadecuadas para aplicar a la ciberdelincuencia. Además, ciertas disposiciones del código penal que son aplicables a delitos cometidos fuera de una red de computadoras podrían no aplicarse fácilmente a la conducta incurrida con el uso de computadoras.

Por el contrario, deberíamos tener cuidado para no tratar los delitos tradicionales como "ciberdelito" simplemente porque la planificación o ejecución implicó el empleo de una computadora. A pesar del uso indebido de una computadora para consumar el delito, cierta conducta culposa podría estar cubierta por normativas generales porque no hay nada particular o singular de un sistema de computadoras en esa conducta. Por el contrario, ciertos delitos cibernéticos son abordados de manera correcta por un instrumento para el combate de la ciberdelincuencia donde, por ejemplo, el uso de una computadora aumenta

- el alcance del delito, por ejemplo, a millares de víctimas o el robo de millones de datos de pago;
- la velocidad del ataque porque una computadora aumenta exponencialmente la capacidad de consumar el delito;
- el grado del daño o la lesión a las víctimas, o
- el anonimato del autor.

Asimismo, con la aplicación de estos conceptos, algunos casos de delitos tradicionales, como las estafas y la explotación de menores, podrían considerarse razonablemente dentro del alcance de la presente negociación. Sin embargo, los Estados Miembros deberían usar criterio en la amplitud del delito cibernético que procuramos abordar a modo de no distorsionar conceptos de larga data de la justicia penal. Normativa e instrumentos penales de larga data no pierden su aplicabilidad solo porque un delito implica algún componente "cibernético".

Un instrumento mundial para combatir la ciberdelincuencia también debería instar a las partes a promulgar legislación que penalice delitos centrales de ciberdelincuencia de una manera tecnológicamente neutra, al tiempo que garantice las salvaguardias procesales. La penalización de los delitos con neutralidad tecnológica (es decir, penalizar la *actividad* que afecta a la confidencialidad, la integridad y la disponibilidad de datos informáticos en lugar de penalizar la *forma* o el *método en particular* que se utilizó, como un ataque por suplantación de identidad o un programa malicioso secuestrador) garantiza que las disposiciones penales sustantivas aborden no sólo las tecnologías actuales y las técnicas delictivas, sino también tecnologías y técnicas futuras. A manera ilustrativa simplemente de la rapidez con que se desarrolla la tecnología, incluso el Estudio preliminar integral sobre ciberdelincuencia de 2013, con su objeto explícito de ser *integral*, careció de detalles sobre tecnologías o técnicas que no se utilizaban ampliamente, o que solo eran emergentes, al momento del estudio, como programas maliciosos secuestradores, la internet de las cosas, criptomonedas y el desarrollo rápido y la prevalencia de la tecnología móvil. En relación con esta inquietud, una de las conclusiones y recomendaciones acordadas por los Estados Miembros del Grupo de Expertos de la ONU fue que "[l]os Estados Miembros deberían velar por que sus disposiciones legislativas resistan el paso del tiempo frente a futuros avances tecnológicos promulgando leyes cuya formulación sea neutral tecnológicamente y que

penalicen las actividades consideradas ilícitas en lugar de los medios utilizados[3]". Esto es de especial importancia en nuestro intento por redactar un instrumento perdurable que aborde suficientemente las tecnologías del futuro y satisfaga las necesidades de los profesionales para el mantenimiento del orden, tanto ahora como en el futuro.

Teniendo en mente estos principios, un instrumento mundial para el combate de la ciberdelincuencia debería incluir la penalización de

- acceso ilegal, es decir el ingreso a una computadora o sistema informático sin autorización;
- interceptación ilegal, es decir, interceptación ilegal en tiempo real del contenido de las comunicaciones o datos de tráfico de las comunicaciones;
- interferencia de datos o sistemas, es decir, programas maliciosos, ataques de denegación de servicio, programas maliciosos secuestradores, eliminación o modificación de datos.
- uso indebido de dispositivos, es decir, tráfico o uso de datos de tarjetas de crédito, contraseñas e información personal que permiten el acceso a recursos;
- delitos relacionados con materiales sobre el abuso sexual de menores;
- delitos relacionados con estafas con el uso de computadoras, es decir la manipulación de sistemas o datos informáticos con fines fraudulentos, como ataques por suplantación de identidad, comprometimiento de correo electrónico comercial y fraude en subastas;

[3] UNODC/CCPCJ/EG.4/2021/2, Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 6 al 8 de abril de 2021, disponible en https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2021/Report/V2102598.pdf,

- delitos relacionados con la contravención de derechos de autor y conexos; y
- disposiciones que aborden tentativa, complicidad y conspiración.

Además, también se debería penalizar el lavado del producto de la ciberdelincuencia. Finalmente, las personas jurídicas deberían estar sujetas a sanciones penales o civiles y administrativas toda vez que participen en los ciberdelitos proscritos por el instrumento.

Fuentes procesales para la recolección y el intercambio de pruebas electrónicas

Además de la penalización de delitos sustantivos, un instrumento mundial para el combate de la ciberdelincuencia debería abordar también la necesidad que tienen las autoridades jurídicas nacionales de preservar, recabar e intercambiar pruebas electrónicas, de manera congruente con el debido proceso y la protección de los derechos humanos y las libertades fundamentales. Algunos Estados Miembros han observado que, en su derecho interno, las fuentes procesales tradicionales tal vez no se apliquen a datos intangibles o tal vez no concedan autorización para la recolección lo suficientemente rápida de pruebas electrónicas volátiles. Desde siempre, legislación desactualizada será insuficiente para responder a los muchos desafíos de las investigaciones de delitos electrónicos, el trabajo con tecnologías novedosas, como servicios generalizados de cifrado y computación en la nube. En consecuencia, las fuentes procesales especializadas para recabar pruebas electrónicas son esenciales. La redacción de estas leyes no debería perder de vista conceptos técnicos aplicables, así como las necesidades prácticas de los investigadores penales. Más específicamente, estas fuentes procesales deberían contemplar

- la preservación acelerada de datos informáticos almacenados;
- órdenes para la presentación de datos informáticos;
- búsqueda y decomiso de datos informáticos guardados;

- recolección en tiempo real de datos de tráfico; y
- recolección en tiempo real de datos de contenido en casos de delitos graves.

Además, el instrumento nuevo debería permitir la cooperación para recabar y obtener pruebas electrónicas para cualquier tipo de delitos, no solo los delitos cibernéticos. Prácticamente todos los delitos penales importantes implican pruebas electrónicas, ya sea en forma de datos telefónicos móviles, correos electrónicos, datos transaccionales u otros datos, que son pertinentes para investigar y judicializar los delitos. Desde el punto de vista nacional, los Estados Miembros necesitan un marco de pruebas legales modernas que permita la admisión de pruebas electrónicas en investigaciones y enjuiciamientos penales, como el intercambio de pruebas electrónicas con fuerzas del orden aliadas a nivel internacional.

Cooperación internacional

Más allá de la legislación interna, la cooperación internacional efectiva en materia de ciberdelincuencia depende de cooperación formal en el marco de tratados, como asistencia jurídica mutua, y de otros medios, como cooperación tradicional autorizada entre policías. El nuevo instrumento para el combate de la ciberdelincuencia debería aprovechar herramientas eficaces para aumentar la cooperación internacional emanada de los tratados en vigor y garantizar que no menoscabe instrumentos en vigor y cooperación internacional en curso en la lucha mundial contra la ciberdelincuencia. Las disposiciones del instrumento para el combate de la ciberdelincuencia respecto de la cooperación internacional, la asistencia jurídica mutua, la extradición, la transferencia del enjuiciamiento, la confiscación de las ganancias, como monedas virtuales y la devolución de los activos confiscados a las víctimas, la doble incriminación y la cooperación de las fuerzas del orden, deberían observar en forma rigurosa las disposiciones de la

UNTOC y UNCAC, como las salvaguardias y protecciones pertinentes en dichos instrumentos, las cuales han sido implementadas satisfactoriamente por la mayoría abrumadora de Estados Miembros de las Naciones Unidas. Además, la disposición sobre asistencia jurídica mutua debería contemplar asistencia amplia para obtener pruebas electrónicas que atañan a un delito penal, ya sea si el delito penal fue cometido o no con el uso de un sistema informático.

Asistencia técnica y fortalecimiento de la capacidad

En los estudios de la UNODC se indica que más del 75% de los países cuentan con una unidad dedicada a las cuestiones relacionadas con la ciberdelincuencia dentro de las organizaciones para el cumplimiento de la ley en funciones, y cerca del 15% cuenta con un organismo especializado dedicado a la ciberdelincuencia. Esto subraya la naturaleza especializada de las investigaciones en materia de ciberdelincuencia, como la necesidad de capacitación especializada. Además, la complexidad de los delitos de ciberdelincuencia y los componentes electrónicos o digitales de los delitos tradicionales creció marcadamente, lo cual impone demandas adicionales para la capacitación y el mantenimiento de investigadores y expertos técnicos altamente capacitados.

La capacidad nacional insuficiente es el motivo más común por el que los países tal vez no cooperen de manera efectiva a nivel internacional. Para la mayoría de los países, la cooperación internacional no fracasa por falta de voluntad, sino por las limitaciones del derecho interno o la experiencia de los organismos del orden. Muchos Estados Miembros no cuentan con los recursos suficientes con respecto a la capacidad de las fuerzas del orden para combatir la ciberdelincuencia o manejar datos electrónicos. Por ejemplo, a la luz de las prioridades nacionales actuales, algunos Estados Miembros se tropiezan con desafíos para formar y conservar a investigadores capacitados, y a examinadores forenses, así como para enfrentar

déficit de equipos y programas informáticos. De este modo, el consenso internacional generalizado apunta a que la asistencia técnica y el fortalecimiento de la capacidad para las instituciones de las fuerzas del orden, los investigadores, los fiscales y los jueces, siguen siendo los requisitos más apremiantes para responder a la ciberdelincuencia en forma eficiente a nivel internacional. Además, a medida que los datos electrónicos se tornan un componente de prácticamente cada tipo de delito, incluso oficiales del orden "no especializados" requerirán cierta comprensión básica de las investigaciones informáticas.

Las disposiciones de un instrumento de ciberdelincuencia respecto de asistencia y capacidad técnicas deberían incluir:

- medidas por los Estados Miembros para iniciar, formular o mejorar programas de capacitación para el personal responsable de la prevención y el combate de la ciberdelincuencia.
- consideración por parte de los Estados Miembros, según la capacidad, para ofrecer mutuamente el mayor grado de asistencia técnica, en especial para beneficio de los países en desarrollo y esos países que podrían enfrentar en forma desproporcionada la amenaza de la ciberdelincuencia en sus respectivos planes y programas a fin de contrarrestarla.
- establecimiento de mecanismos mediante los cuales contribuciones financieras voluntarias de los Estados Miembros respalden la implementación de un instrumento de ciberdelincuencia.
- consideración por los Estados Miembros de contribuciones voluntarias a la Oficina de las Naciones Unidas contra la Droga y el Delito y el Programa Mundial contra el Delito

Cibernético y sus labores conexas para el fortalecimiento de la capacidad de la justicia penal.

Participación de la sociedad, las entidades y las organizaciones públicas

El combate de la ciberdelincuencia no puede ser un esfuerzo aislado a la luz de su complejidad y naturaleza multifacética. Un instrumento para el combate de la ciberdelincuencia debería tener en cuenta la importancia de la participación activa por parte de individuos y grupos, con el debido respeto por la paridad de género, como organizaciones no gubernamentales, organizaciones de la sociedad civil, instituciones académicas y el sector privado en la prevención de la ciberdelincuencia. Dicha participación tiene la posibilidad de generar concientización pública sobre las amenazas de la ciberdelincuencia; garantizar que la tarea de los Estados Miembros se realice en forma transparente; y abordar asuntos sustantivos relacionados con la privacidad, las libertades civiles y los derechos humanos. Además, un instrumento efectivo depende de las contribuciones de individuos y entidades con experiencia en el campo de la ciberdelincuencia. A fin de poner en marcha un instrumento práctico y efectivo para el combate de la ciberdelincuencia, resulta esencial contar con la participación robusta de expertos en la materia.

Mecanismos de aplicación

La determinación de la necesidad o no de un proceso separado para analizar la aplicación futura del instrumento y, en tal caso, la forma que adoptará, es demasiado preliminar en esta etapa. Hay varios modelos exitosos para tener en cuenta. A la luz del déficit de recursos disponibles para asistencia técnica, se deberían considerar métodos que dependen de opciones acordes a los presupuestos para aprovechar al máximo las contribuciones de donantes para la

asistencia técnica. Un método de este tipo sería autorizar a la Comisión de Prevención del Delito y Justicia Penal, establecida por la Resolución 1992/1 del Consejo Económico y Social, a considerar todos los asuntos relativos a las metas del instrumento para el combate de la ciberdelincuencia. Existe un precedente exitoso para dicha supervisión en la Comisión de Estupefacientes, que vela por los tres tratados internacionales para el control de los estupefacientes. Conforme se esboza en la sección *Participación de la sociedad, las entidades y las organizaciones públicas*, resulta esencial considerar la participación robusta de la sociedad, las entidades y las organizaciones públicas al momento de plasmar en el terreno de la práctica todo trabajo emanado de un instrumento. Sin embargo, se debería reservar el debate sobre los mecanismos de aplicación hasta definir mejor el alcance del instrumento.