POSICIÓN PRELIMINAR DE COLOMBIA
SOBRE ALCANCE, OBJETIVOS Y ESTRUCTURA
DEL FUTURO CONVENIO A SER NEGOCIADO
EN EL MARCO DE LAS NACIONES UNIDAS,
CONTRA LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES CON FINES DELICTIVOS
(5 de noviembre de 2021)

Habida cuenta de la aprobación de la Resolución 74/247 de la Asamblea General de las Naciones Unidas, por medio de la cual se estableció un Comité intergubernamental especial de expertos de composición abierta para elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones (TICs) con fines delictivos, y considerando la invitación de la Presidente del Comité Ad Hoc para que los Estados Miembros presenten posiciones nacionales sobre el alcance, los objetivos y la estructura que debería tener el futuro Convenio sobre el delito cibernético, a continuación, nos permitimos remitir los comentarios preliminares por parte de Colombia:

- **ALCANCE:**

El nuevo convenio debería centrarse en la búsqueda de una herramienta de cooperación jurídica internacional para la prevención, la investigación, el juzgamiento y la sanción de los delitos cibernéticos por las autoridades nacionales y lo relacionado con las evidencias electrónicas. Por lo tanto, se deben evitar discusiones que no se centren en el problema jurídico de la cibercriminalidad y la gestión de las evidencias electrónicas.

Deben evitarse discusiones sobre temas que puedan ser políticamente álgidos y que no se refieran directamente al núcleo del convenio a negociar.

Se considera fundamental que la nueva convención tenga en cuenta los marcos e instrumentos jurídicos internacionales existentes, entre los que se encuentran la Convención de las Naciones Unidas sobre la Delincuencia Organizada Transnacional (UNTOC), la Convención de las Naciones Unidas contra la Corrupción (UNCAC) y la Convención de Budapest sobre la Ciberdelincuencia, dado que la legislación nacional y las prácticas de la mayoría de los Estados están conforme o se sustentan en los acuerdos

existentes, por lo cual, los estándares futuros deben ser compatibles con estos. Asimismo, se debe garantizar que no se desarrollen normas que generen conflicto o riñan con otras obligaciones internacionales adoptadas por los Estados.

En ese sentido, el convenio debe tener un enfoque complementario, es decir, que la negociación debe considerar, en principio, el trabajo que la comunidad internacional ya viene realizando desde hace algunos años en la lucha contra el cibercrimen y no contradecir las diferentes obligaciones internacionales aplicables de los respectivos Estados. Por lo tanto, se debe aprovechar las potencialidades y los avances que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional ha traído en materia dogmática y de herramientas de cooperación judicial.

Deben tenerse en cuenta los marcos multilateral, regional y bilateral actualmente vigentes en materia de asistencia judicial mutua, a fin de evitar posibles conflictos normativos, complementar y utilizar los instrumentos internacionales ya existentes y no obstaculizar su efectiva aplicación. Así, debe recomendarse no solo la consideración exhaustiva de antecedentes multilaterales como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia, sino también los acuerdos bilaterales y regionales, como es el caso de la Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Específicamente, debe tenerse en cuenta el Convenio sobre la Ciberdelincuencia (Budapest, 2001), ya que incluye conceptos ampliamente debatidos y una experiencia fáctica internacional de veinte años. Su no observación traería consigo el riesgo de entrar en un camino que contravenga los avances ya obtenidos en la lucha contra la cibercriminalidad.

Asimismo, el proceso debe considerar los resultados del trabajo del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético en el marco de las Naciones Unidas, y aprovechar el listado de conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos.

Resaltamos la importancia de que la elaboración de la nueva convención se realice de forma inclusiva, transparente y -hasta donde sea posible, se base en el consenso, así como se llevaron a cabo los anteriores procesos de las Naciones Unidas para concertar la Convención contra la Delincuencia Organizada Transnacional y la Convención contra la Corrupción, para contribuir a prevenir futuras controversias en la materia.

➢ **OBJETIVO:**

El objetivo general de la Convención debería ser la adopción de un marco de cooperación internacional en materia de justicia para la prevención, investigación y persecución integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones (TICs) con fines delictivos, la cibercriminalidad, y lo relacionado con las evidencias electrónicas.

➢ **ESTRUCTURA:**

- Línea base de definiciones y conceptos tecnológicos estandarizados y con vocación de permanencia en el tiempo.

- Disposiciones sustantivas (tipos penales que sean adoptados en las legislaciones nacionales).

  En tal sentido, la Convención debería dar relevancia penal a un conjunto de conductas que afectan la información y los sistemas informáticos.

  Parece razonable centrarse por orden dogmático y metodológico, exclusivamente sobre los llamados delitos núcleo de la cibercriminalidad; Delitos de acceso informático no autorizados a redes o sistemas informáticos a través del delito de acceso abusivo a un sistema informático; El espionaje informático, que asocia todas las conductas que vulneren la intimidad de personas naturales y jurídicas a través de la interceptación u obtención de datos, comunicaciones, archivos o bases de datos almacenadas en sistemas informáticos o transmitidos a través de redes de comunicación y que encierra los delitos de Interceptación de datos informáticos, la violación de datos personales y la suplantación de sitios web para capturar datos personales; El sabotaje informático, orientado a la obstaculización, daño, inutilización, supresión, interferencia o inutilización de sistemas informáticos, bases de datos o procesos de tratamiento, transferencia y transmisión de datos y que incluye los delitos de obstaculización ilegítima de sistema informático o red de telecomunicación.

  De otra parte, se podrían incluir algunas conductas que, por cometerse a través de medios informáticos, tienen un fuerte impacto, alcance y su investigación encierra cierta complejidad, de manera que el instrumento sea lo suficientemente flexible como para servir de herramienta para combatir actividades ilegales conexas con otros delitos.

- Cláusula de doble incriminación: este mecanismo es importante con miras a lograr prestar la asistencia judicial recíproca, independientemente de que el hecho que la origine no sea punible según la legislación del Estado requerido, garantizando, así, entre otros aspectos, que los ciberdelincuentes no encuentren refugios seguros en algunos países, por la ausencia de una legislación estándar común.

- Disposiciones procesales que permitan hacer efectiva la cooperación jurídica: en tal sentido, se considera imperativo intensificar la cooperación internacional para la investigación de los delitos cibernéticos, en especial frente a la gestión de pruebas digitales, cadena de custodia, conservación de datos y análisis forense. La transmisión y almacenamiento de datos es un asunto que requiere atención urgente, así como la definición de mecanismos que permitan la comunicación y respuesta rápida entre autoridades homólogas de los diferentes Estados, a través de canales digitales apropiados y seguros.

- Agravantes de las conductas que afectan el bien jurídico de la protección de la información y de los datos, como aquellas relacionadas con captura masiva de datos personales, violación de derechos humanos, o aquellas que tengan como blanco infraestructuras críticas y servicios esenciales.

- Cooperación judicial internacional: facilitar, ampliar y agilizar las solicitudes de asistencia legal mutua (MLAs), a través de canales digitales, con las seguridades que correspondan, y a través de formatos estándar.

- Definir mecanismos investigativos especializados en la recolección de evidencia digital, especialmente en lo relacionado con la evidencia que se encuentre almacenada en diferentes jurisdicciones.

- Es importante que los Estados Miembros acuerden mecanismos que garanticen un nivel adecuado de protección de datos personales en el intercambio de información a través del instrumento internacional, no solo por la relevancia que en el entorno digital ha tomado actualmente la protección de los datos personales, sino, también, para evitar que las normas particulares de cada país puedan constituir eventualmente un obstáculo para el intercambio efectivo de información entre los Estados.

- Estímulo a la asistencia técnica, la divulgación de conocimientos y buenas prácticas relacionados con la investigación, judicialización y sanción. Adicionalmente, para

acortar la brecha digital, se considera fundamental que incluya el fortalecimiento de capacidades a instituciones encargadas de hacer cumplir la ley y otras autoridades de justicia nacionales, especialmente en lo referente a los programas de educación y entrenamiento como una forma de prevención.

Impulsar, a través de escuelas de capacitación regionales, la cooperación técnica. Dada la complejidad y la especificidad en la investigación de crímenes cometidos a través de medios informáticos y que no permiten investigar eficazmente, es necesario brindar capacitación especializada a los fiscales e investigadores de una manera organizada y continua, estableciendo previamente planes de trabajo con resultados esperados.

- Se resalta que la promoción de la cooperación sólida y basada en la confianza entre los sectores público y privado en el ámbito de la ciberdelincuencia es un tema de la mayor importancia, por lo cual resulta fundamental tener una posición consistente en el tema, y que se facilite la obtención de evidencia digital por parte de actores en el entorno digital, incluyendo a las empresas prestadoras de servicios de internet (ISPs) y comunicaciones.

- Promover y facilitar el acceso de autoridades a plataformas colaborativas para el fortalecimiento de capacidades e intercambio de información, así como a herramientas de análisis y contexto, para las investigaciones en esta materia.

- Disposiciones que faciliten el acceso a información expedita en casos de emergencia.

- Finalmente, se sugiere incluir la creación de una red de Puntos de Contacto (PoC) con atención permanente (24 horas / 7 días a la semana) para la atención de las solicitudes de cooperación jurídica internacional en la materia, que adicionalmente podría complementarse con una red de contactos para: i) potenciar el intercambio de conocimientos y experiencias en materia de ciberdelitos y delitos conexos; ii) crear y divulgar las buenas prácticas iii) optimizar y agilizar la cooperación judicial internacional entre los distintos países.

……