RELACIONES EXTERIORES
SECRETARÍA DE RELACIONES EXTERIORES

Elementos de posición del Gobierno de México para el Comité de Naciones Unidas encargado de elaborar una Convención contra la Ciberdelincuencia

Para el Gobierno de México las tecnologías de la información y telecomunicaciones, las plataformas digitales y el entorno cibernético, ofrecen grandes oportunidades para potenciar el desarrollo, cerrar brechas de desigualdad, promover la inclusión, el bienestar, la justicia y los derechos.

Al mismo tiempo, México reconoce que la comisión de delitos y la propagación de un mercado ilícito mediante estas tecnologías representan una preocupación creciente para gobiernos, empresas, organizaciones sociales y todas las personas.

La cooperación internacional y los mecanismos de asistencia jurídica e intercambio de información son más necesarios que nunca. México apuesta por el multilateralismo, y en especial por el papel de las Naciones Unidas, para generar respuestas integrales y significativas ante este reto global.

México considera que el mandato generado por la Asamblea General para la elaboración de una Convención integral contra el uso de las tecnologías de la información con fines delictivos, constituye una oportunidad idónea para lograr un proceso sustantivo, comprometido, plural, incluyente y transparente, y que se alimente de las lecciones aprendidas de otros procesos de Naciones Unidas relacionados con el tema, y de otras experiencias regionales vinculadas.

A continuación se presentan los aspectos que el Gobierno de México esperaría que marcaran el proceso de elaboración y los contenidos de la futura Convención.

Enfoque, alcances y tipo de Convención.

La Convención debe ser un instrumento jurídico vinculante integral, que contemple aspectos sustantivos y procesales, orientado a establecer bases para la cooperación internacional y el intercambio de información, experiencias, capacidades y mejores prácticas.

Se espera que contribuya a promover estándares para mejorar la investigación, mitigación y judicialización. Se espera que si bien la Convención no excluya la posibilidad de suscribir otros instrumentos internacionales en la materia, sea referente para contar con un esquema homologado que haga más eficiente la persecución de los ciberdelitos.

Se considera que debe incorporar:

- Definiciones generales, tipologías básicas y actores competentes.
- Medidas procesales básicas con las que deberán contar los Estados para la adecuada investigación y persecución de los delitos cibernéticos.
- Tipos penales generales que debieran ser considerados por las respectivas legislaciones nacionales.
- Mecanismos de acceso a la información y de fomento a la colaboración operativa.

También se considera conveniente que la futura Convención permita la formulación de reservas y de declaraciones interpretativas, que contenga un procedimiento de enmienda ágil para facilitar su actualización y que establezca mecanismos para dirimir controversias. Será conveniente que la entrada en vigor se supedite al depósito de 50 instrumentos de ratificación.

Con la certeza del contenido de la Convención, será oportuno acordar un mecanismo eficiente de examen de la implementación, universal, entre pares y no oneroso.

Relevancia de otros instrumentos internacionales.

Para el gobierno de México es importante que la Convención parta de la afirmación de que el Derecho Internacional es aplicable al ciberespacio, y que por ello se tomen en consideración desarrollos existentes en diversos instrumentos jurídicos internacionales, tales como:

- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus tres Protocolos complementarios.
- Estatuto de la Corte Internacional de Justicia.
- Convenio contra la Ciberdelincuencia del Consejo de Europa.
- Tratados sobre protección y flujo transfronterizo de datos personales.
- Tratados internacionales en materia de derechos humanos, y aquellos que salvaguardan las garantías de las personas que intervienen en procesos jurisdiccionales.
- Tratados aplicables a la propiedad intelectual.
- Tratados bilaterales en materia de extradición, asistencia jurídica mutua en materia penal y otras formas de cooperación jurídica internacional.

Se valora también que para el proceso de negociación sirvan de guía documentos adoptados en el seno de la ONU y otros foros internacionales relevantes, principalmente:

- Recopilación de conclusiones y recomendaciones surgidas de las reuniones del Grupo Intergubernamental de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético de 2018, 2019 y 2020.
- Informe Final del Grupo de Expertos Gubernamentales (GGE) para avanzar el comportamiento responsable de los Estados en el ciberespacio de 2019-2021, y los informes previos de 2013 y 2015.
- Informe Final del Grupo de Composición Abierta (OEWG) sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional de 2019-2021.
- Proyecto de directrices para la utilización de la Agenda sobre Ciberseguridad Global (ACG) que elaboró la Unión Internacional de Telecomunicaciones (UIT).
- Resoluciones de la Asamblea General de la ONU sobre el Derecho a la privacidad en la era digital.
- Resoluciones del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en internet.

Delitos cibernéticos/conductas delictivas que debieran ser abordados:

Para el gobierno de México la Convención debe enfatizar aquellas conductas reconocidas por el derecho internacional como ilícitas (en los términos previstos en otros tratados adoptados en el marco de las Naciones Unidas), que se realicen por medios electrónicos.

No se espera que la Convención incluya un catálogo exhaustivo de delitos, ni que todas las tipologías se homologuen a los distintos sistemas jurídicos, pero sí es recomendable que en el proceso de elaboración se genere un diálogo como referente general para los siguientes casos:

- Robo y suplantación de identidad.
- Fraude y extorsión.
- Secuestro de información (*ransomware*).
- *Malware* y conductas delictivas relacionados con la producción, almacenamiento, distribución, comercialización y ejecución de códigos maliciosos.
- Exposición de información personal o institucional en perjuicio de sus propietarios.
- Delitos relacionados con tráfico y trata de personas, pornografía infantil y violaciones a la

intimidad sexual.
- *Grooming* y acoso cibernético.
- Violencia digital, incluyendo de género y por motivos de odio, racial, de nacionalidad, religión u hostilidad política.
- Vectores de ataque (*phising, vishing, smishing, pharming*).
- Delitos contra la soberanía nacional, tales como terrorismo, sabotaje, espionaje e intrusión en los sistemas con información reservada por motivos de seguridad nacional.
- Actos delictivos contra infraestructuras críticas de información y contra la confidencialidad, integridad y disponibilidad de la información.
- Delitos en contra de niños, niñas y adolescentes.
- Violación de la libertad de expresión.
- Delitos cometidos contra la propiedad intelectual.
- Delitos contra el sistema financiero.
- Venta ilegal de armas, animales, medicamentos controlados y aquellos que no cuentan con registro sanitario.
- Falsificación de moneda y de documentos oficiales.
- Uso de criptodivisas y de bienes de uso dual con fines delictivos.
- Modificación ilegal de portales (*Defacement*).
- Responsabilidad de las personas jurídicas.

Se considera oportuno que se discuta también, al elaborar la Convención, si se admitirá la sanción a la realización de delitos en grado de tentativa, así como de determinantes que agraven el acto delictivo e incrementen las penas.

Aspectos relacionados con la soberanía y jurisdicción:

- Reafirmar el respeto a la soberanía nacional y el principio de no intervención en los asuntos internos de cada Estado.
- Establecer reglas generales para la determinación de la jurisdicción aplicable, tomando como referente disposiciones similares de otros instrumentos jurídicos y procesos.
- Generar medidas comunes para la obtención de datos de tráfico y de contenido, y que prevengan la intercepción o bloqueo ilegal de datos.
- Avanzar mecanismos que den certeza a la obtención y conservación o preservación de las evidencias digitales, así como de su entrega.
- Aclarar diligencias de investigación como citaciones o aprehensiones.
- Elaborar especificaciones para la entrega de datos técnicos y de contenido en investigaciones criminales, y para la divulgación rápida de datos informáticos.
- Abordar la obligación legal de los operadores de tecnología, prestadores de servicios y contenidos en internet para entrega de información a las autoridades competentes durante la investigación, independientemente de su localización física.

Aspectos sobre intercambio de información y cooperación internacional:

Para el gobierno de México, la Convención deberá tener como uno de sus principales propósitos generar certezas para el intercambio de información y la cooperación internacional, y establecer procesos para su ejecución eficaz. Se espera que se aborden, entre otros aspectos:

- Asistencia jurídica mutua.
- Extradición.
- Mecanismos comunes para la solicitud, respuesta, recepción e intercambio de información para la investigación y con fines de inteligencia.
- Procedimientos de control judicial que permitan una colaboración ágil y efectiva durante la

investigación.
- Cooperación para la realización de diligencias de investigación policial y obtención de testimonios para los procesos judiciales, considerando también el uso de las tecnologías de la información y comunicación.
- Elaboración de guías, estándares, metodologías y mejores prácticas para la prevención e investigación de delitos cibernéticos.
- Fomento de la colaboración entre CERT o CSIRT Nacionales para la prevención de los delitos cibernéticos.
- Investigaciones coordinadas.
- Recomendar un marco común mínimo para la protección de la información y la transparencia, para que a pesar de las distintas políticas que a nivel nacional tiene cada Estado, se puedan compartir datos de investigaciones y procesos judiciales.
- Establecer plazos mínimos para la conservación de datos y la preservación de pruebas digitales.
- Recomendar reglas y términos a los cuales habrán de sujetarse las acciones de intervención de las comunicaciones privadas y la geolocalización en tiempo real.
- Establecer parámetros generales para el respeto y regulación de las políticas de privacidad.
- Promover la homologación de estadísticas locales, regionales y globales.

Aspectos relacionados con protección y ejercicio de derechos humanos:

Todas las medidas a instrumentar desde la futura Convención deberán ser consistentes con las obligaciones contenidas en los instrumentos internacionales de derechos humanos. Se espera además que sus disposiciones sean compatibles con las normas relativas a la libertad de expresión.

El gobierno de México espera que en el proceso de elaboración de la Convención se aborden:
- Conceptos y desarrollos relativos a empresas y derechos humanos.
- Privilegiar la investigación, persecución y castigo de la violencia de género, y de delitos contra niñas, niños y adolescentes a través de Internet.
- Promover la investigación, persecución y castigo de conductas racistas, que inciten a la violencia, exclusión o segregación de las personas.
- Elementos comunes mínimos acerca de la neutralidad de la red.
- Recomendar mecanismos para la protección de la información por parte de empresas de servicios de Internet.

Elementos relacionados con fortalecimiento de capacidades y asistencia técnica:

El gobierno de México considera que para la instrumentación eficaz de la futura Convención, será necesario establecer disposiciones que promuevan el fortalecimiento de capacidades, tanto para la prevención como para la persecución de los delitos cibernéticos. Será conveniente:
- Avanzar esfuerzos de capacitación, asistencia técnica y mejores prácticas, así como procedimientos estandarizados para realizar forensia informática y obtener evidencia digital válida.
- Promover iniciativas de educación para la prevención y campañas públicas replicables de concientización.
- Fomentar también la creación o fortalecimiento de CERTs en sectores diversos, tales como, financiero, académico, comercial y energético.
- Elaborar guías, lineamientos y recomendaciones que impulsen la adopción de mejores prácticas.
- Ampliar el catálogo de capacitaciones enfocadas a distintos grupos interesados: investigadores, fiscales, jueces, diplomáticos, legisladores, y actores no estatales.

Aspectos sobre participación de actores no estatales relevantes (sociedad civil, sector privado, academia):
Para el gobierno de México resulta conveniente que desde el proceso mismo de elaboración de la Convención se busquen mecanismos para facilitar la participación y la aportación de insumos de organizaciones de la sociedad civil, sector privado, proveedores de servicios, y de la academia y centros de investigación. Será deseable que se considere: • El posible involucramiento de estos actores en los procesos para prevenir y luchar contra los delitos cibernéticos. • Promover entornos colaborativos con CERTs privados, *Carriers* y empresas diversas de telecomunicaciones. • El diálogo con la iniciativa privada que opera infraestructuras críticas de información o que están dentro de los sectores estratégicos, así como con empresas proveedoras de servicios gratuitos de Internet como correo electrónico, mensajería instantánea, micro-blogs y servicios de transporte en línea. • Apoyar medidas de autorregulación y conciencia social, así como promover la inclusión de los conceptos de empresas y derechos humanos.