31° Periodo de Sesiones de la Comisión de Prevención del Delito y Justicia Penal

Intervención de México

Debate temático: Fortalecimiento del uso de pruebas digitales en la justicia penal y la lucha contra el delito cibernético, en particular en lo que respecta al abuso y la explotación de menores en actividades ilegales con el uso de Internet

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.

El confinamiento por la pandemia llevó a un incremento notorio de los usos delictivos de las plataformas cibernéticas, y en especial de casos de explotación sexual infantil. Dado el fácil traspaso de las fronteras físicas por estas actividades ilícitas resulta prioritario fortalecer la cooperación penal en cuanto a recolección, manejo y resguardo de las pruebas digitales. Con base en la experiencia nacional reciente, México propone hoy:

1. **Fortalecer alianzas público-privadas** con los proveedores de servicios y contenidos de Internet, **que reconozcan la aportación estratégica que la conservación y la entrega de datos tienen en la investigación criminal**, a partir de lineamientos claros y homologados para el acceso transfronterizo y la colaboración con los proveedores de servicios y de comunicaciones.
2. **Diseñar un protocolo y medidas de autenticación y compartición de evidencia digital** alojado en la nube, para que cada país, a través de sus instituciones de justicia, facilite el acceso a elementos para las investigaciones penales, bajo un espíritu de cooperación.
3. **Generar una norma o estándar internacional en materia de cooperación y colaboración con la justicia** basado en las mejores prácticas internacionales para obtener y garantizar la conservación o preservación de la información por parte de los proveedores.
4. La **admisibilidad de las pruebas electrónicas** debe privilegiar el enfoque neutral de la tecnología para evitar la discriminación de dichas pruebas (nacional/internacional), y dicha admisibilidad deberá estar fundada en la garantía de **mismidad** (*sameness*) **y autenticidad** de dichos indicios para que reflejen la **continuidad y la trazabilidad** dentro de la cadena de custodia al incorporarlos como pruebas en el proceso penal.
5. Reconocer la existencia de **factores no considerados en la obtención y presentación de las pruebas electrónicas**, tales como el almacenamiento en la nube, el servicio de terceros y la distribución de los datos, que hacen necesario considerar la creación de directrices no existentes hasta el momento para los casos de la evidencia digital que esté almacenada en alguno de los esquemas mencionados.

Las deliberaciones de este debate temático revisten particular relevancia, a la luz de los trabajos en marcha del *Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos*.

México considera que el mandato generado por la Asamblea General para la elaboración de esta Convención 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.

Para concluir, y como resultado de los esfuerzos para fortalecer sus capacidades nacionales en materia de ciberseguridad, el gobierno de México desea compartir que ha elaborado e implementado un **Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos,** que busca gestionar de forma coordinada los incidentes cibernéticos de mayor criticidad e impacto en activos esenciales de información, mediante la aplicación de procedimientos y de mejores prácticas de ciberseguridad, para la contención y mitigación de amenazas cibernéticas, a fin de mantener niveles de riesgo aceptables en las dependencias federales, entidades federativas, organismos constitucionales autónomos, academia e instancias del sector privado del país.

Muchas gracias.