COMENTARIOS DEL GOBIERNO DE MÉXICO AL "ESTUDIO EXHAUSTIVO SOBRE EL PROBLEMA DEL DELITO CIBERNÉTICO"

Ciudad de México, a 31 de agosto de 2016

El Gobierno de México reconoce el esfuerzo de los expertos y del Secretariado de la Oficina de las Naciones Unidas contra la Droga y el Delito para la integración de este estudio, que puede considerarse un documento de referencias generales y estadísticas valioso, pero de ningún modo una guía para las decisiones de los Estados en materia de políticas públicas nacionales para hacer frente al ciberdelito.

Aunque la información integrada por la Oficina de las Naciones Unidas contra la Droga y el Delito deriva del cuestionario aplicado previamente a los países participantes, no se hacen alusiones específicas a las mejores prácticas de muchos países o su situación normativa frente a ciertos delitos cibernéticos. Sin embargo, la articulación general del texto permite orientar mejor las discusiones sobre el fomento de la cooperación internacional como elemento clave.

Para el Gobierno de México, es de gran relevancia subrayar que el alcance del mandato de la ONUDD y de la Comisión de Prevención del Delito y Justicia Penal (CCPCJ), que se concentra en la asistencia técnica y la cooperación internacional, queda bien reflejado en el Estudio. Sería deseable, que se conminara a los Estados a compartir información con el Secretariado sobre nuevos programas o medidas de asistencia técnica y fortalecimiento de capacidades que emprendan a nivel bilateral, regional o mediante otros foros, a fin de alimentar el compendio de experiencias para futuras discusiones.

Si bien el estudio lleva por título Estudio Exhaustivo, el Gobierno de México considera que no es conveniente considerarlo así, toda vez que no se incluyeron análisis más sustantivos sobre tendencias regionales particulares o sobre la naturaleza cambiante de la comisión de delitos que recurren al uso de las plataformas cibernéticas.

El citado documento ya se encuentra publicado en internet y su revisión en este momento si bien implica únicamente la validación de la información reportada a 2013, ésta ya se encuentra desactualizada, toda vez que han evolucionado los marcos normativos de los diversos países e incluso de los instrumentos de cooperación internacional suscritos, como es el caso del "Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia" de la Conferencia de Ministros de Justicia e Iberoamérica (COMJIB), mismo que establece líneas de acción y cooperación mutua entre 21 países iberoamericanos contra la delincuencia en el ciberespacio.

Los tipos de delitos contenidos en el Estudio tienen hoy nuevas expresiones e incluso existen algunos diagnósticos sobre la presencia de nuevos comportamientos delictivos en la red. Sin embargo, tampoco se esperaría que se generara una lista exhaustiva, ya que la naturaleza cambiante del uso de las tecnologías de la información y la comunicación, conducen al desarrollo de técnicas mejoradas para vulnerar la información, diversificar y por lo tanto fortalecer acciones criminales y terroristas que utilizan Internet para el robo de información y cometer desde los delitos cibernéticos más comunes como el phishing, fraude a tarjetas de crédito o robo de identidad.

Por otro lado, vale la pena destacar que no se menciona el concepto de Deep Web ni Dark Web, como canales ilícitos que ofrecen anonimato a los criminales para la venta de drogas, armas, tráfico de personas, bases de datos confidenciales y otros delitos, así como tampoco las transacciones con criptomonedas como el Bitcoin son un referente del estudio, a pesar de que su uso se ha incrementado.

El análisis que se obtiene del Estudio acerca de técnicas de investigación, obtención de pruebas y atribución de responsabilidad legal, que sin duda cae en la jurisdicción de cada Estado, debe evitar ser redactada como recomendaciones a implementar, toda vez que no es un análisis exhaustivo y que los mismos asuntos se discuten en otros foros dentro del Sistema de Naciones Unidas pero con mandatos más específicos.

La participación de los CERT ha crecido en los últimos años en cuanto a la coordinación para atención de incidentes cibernéticos y se ha generado estrategias nacionales de ciberseguridad, mismas que no son referidas. Además, sobre el tema de infraestructuras críticas no mencionan los organismos ni las políticas específicas generadas para la protección de las infraestructuras críticas en diversas regiones del mundo.

Finalmente, se comenta que aunque a lo largo del estudio se desprenderían algunas referencias sobre la importancia del intercambio de experiencias con el sector privado y las organizaciones de la sociedad civil, para el Gobierno de México sería conveniente que las alusiones fueran explícitas y más concretas, para hacer incluso una invitación a recibir información sobre los mecanismos existentes en diversos países y regiones, sobre la manera de conciliar visiones y materializar apoyos entre los sectores público y privado para responder al delito cibernético.