Algunas líneas generales

Segunda Sesión de la Comisión Ad Hoc sobre el Uso de las Tecnologías de la Información y la Comunicación – TIC- con fines delictivos

Viena - Austria

COSTA RICA

- La creación de un nuevo instrumento convencional en materia de ciberdelincuencia

La ciberdelincuencia es, por su naturaleza, un fenómeno transnacional. Los anquilosados y decimonónicos conceptos de Estado-Nación y soberanía sobre los cuales se ha cimentado el Derecho Penal y Procesal Penal, resultan insuficientes para contrarrestar conductas que pueden ser desplegadas desde cualquier punto del planeta, e incluso fuera de él. En línea con lo anterior, el Estado costarricense se muestra complacido con la idea de promover un convenio en el marco del sistema universal de la Organización de las Naciones Unidas.

Ahora bien, en virtud del carácter técnico que viene aparejado al fenómeno de la ciberdelincuencia y el impacto que tiene el uso de las tecnologías en la ejecución y facilitación de este tipo de criminalidad, se estima necesario que la regulación transnacional cuente con el criterio de expertos forenses en la materia, a fin de incorporar los términos y procedimientos técnicos que permitan regular de manera general temas como la investigación especializada, la incorporación del material probatorio, la incautación de evidencia, las medidas procesales preventivas para salvaguardar datos, entre otros, sin agotar o limitar su contenido, teniendo en cuenta el avance vertiginoso y la innovación constante de las tecnologías digitales.

Debe tenerse claridad que en temas de ciberdelincuencia la cooperación y asistencia internacional son esenciales. Es imperativo que los Estados puedan recopilar, compartir e intercambiar información sobre el fenómeno y brindarse

auxilio mutuo a través de sus experiencias, generando así espacios de capacitación que les permitan abordar de forma conjunta y coordinada las nuevas tendencias de la ciberdelincuencia, así como aplicar y mantener en revisión constante las metodologías comunes utilizadas en la persecución criminal de estas figuras.

La protección y el establecimiento de mecanismos de asistencia a las víctimas y testigos de la ciberdelincuencia es relevante, toda vez que en muchas oportunidades no solo se vislumbra una pérdida patrimonial como consecuencia de estos fenómenos delictivos, sino que se afectan bienes jurídicos de diferentes órdenes, tales como la integridad, la dignidad humana, la autodeterminación sexual, la intimidad, las comunicaciones, entre otros. Por ende, la regulación de las herramientas para la protección de las víctimas que cada Estado desarrolla en sus ordenamientos jurídicos internos debe venir acompañada y complementada con mecanismos de cooperación, y asistencia multilateral internacional que permitan garantizar una protección efectiva, asesoramiento técnico y jurídico, información, así como medidas concretas para aminorar los efectos y consecuencias adversas que la ciberdelincuencia puede provocar en esas víctimas y testigos.

La ciberdelincuencia tiene un amplio espectro en cuanto a las víctimas que afecta. Los ataques de esta naturaleza se dirigen no solo contra personas físicas en particular, sino también contra empresas públicas y privadas. Incluso son notorios los casos de Estados que, como un todo, han sido agredidos desde un punto de vista cibercriminal. El caso de Estonia (2007) es paradigmático en esta materia. Tristemente, nuestro país Costa Rica es víctima actual de furibundos ciberataques, los cuales incluyen el daño informático y el sabotaje informático (*ransomware)*. Los efectos macro de estos crímenes son incalculables. En Costa Rica la afectación ha incluido el entorpecimiento para el desalmacenaje aduanal de diversos productos importados, así como la imposibilidad para pagar su salario de manera puntual a educadores y educadoras, por citar tan solo dos ejemplos.

Al hablarse de ciberespacio o cibercrimen, es inevitable la referencia a conceptos como redes sociales digitales, criptoactivos, entre otros. Bajo esta inteligencia, las diferentes plataformas digitales y redes sociales si bien se han convertido en un instrumento importante para la economía, agilizando el comercio de productos y servicios, también se ha convertido en una herramienta que ha venido a facilitar la comisión de hechos delictivos, que se adentran en el flujo comercial de las redes y diferentes plataformas y que representan una alternativa viable para el tráfico ilícito de mercancías y hasta de personas. A manera de ejemplo, según informa la Agencia EFE, recientemente, la Junta Internacional de Fiscalización de Estupefacientes JIFE, que es un órgano semi judicial encargado de velar por el cumplimiento de los tratados internacionales sobre drogas, de la ONU, advierte en su informe anual que las plataformas digitales se han convertido en nuevos medios para la compra de sustancias estupefacientes y además para la promoción entre las poblaciones jóvenes de conductas inadecuadas asociadas al consumo de este tipo de sustancias ilícitas. Particularmente, se ha identificado que mediante plataformas digitales como *Snapchat*, *Instagram* y otros sitios de la *Deep Web* se ha incrementado el comercio de sustancias tales como cannabis, analgésicos y fentanilo. Todo lo anterior pone en evidencia la necesidad de incluir dentro del convenio figuras base para punir las nuevas modalidades de delincuencia que hacen uso de las tecnologías de la información para facilitar su ejecución, y llegar de forma masiva a los destinatarios.

Además, mediante el uso aún más generalizado de las criptoactivos se agilizan las transferencias y transacciones para la comercialización de mercancías de forma ilícita, mecanismo que permite ocultar el origen ilícito de los fondos y que impide en muchas ocasiones identificar a los responsables directos de tales delincuencias.

Por otra parte, la UNODC[1] reporta que la internet ha facilitado la actividad de crimen organizado relacionado con la trata de personas y el tráfico ilícito de migrantes de distintas maneras: comunicación entre los integrantes de la

[1] (https://www.unodc.org/documents/e4j/tip-som/Module_14_-_E4J_TIP-SOM_ES_FINAL.pdf)

organización, acoso en línea, reclutamiento de víctimas en línea, pagos en línea por servicios de explotación, entre otros.

-***La dignidad de la persona humana como eje de la tutela penal también en materia de ciberdelincuencia***

Al cuestionarse sobre la justificación para tipificar delitos relacionados con la discriminación, el racismo o la xenofobia, así como otros conexos, es fundamental partir del concepto de dignidad humana como referente axiológico. Indudablemente, las tecnologías de la información representan un importante amplificador de conductas que, si bien son tan antiguas como la vida social (piénsese, a modo de ejemplo, en la difusión de discursos de odio, la negación de la condición de persona a ciertos colectivos, entre otros) cuentan hoy con la posibilidad de ser desplegadas con inmediatez y a una escala masiva. Basta reflexionar acerca de las redes sociales como plataformas desde las cuales se propaga la desinformación o el odio hacia ciertos segmentos del tejido social.

La negación de los derechos fundamentales a cualquier ser humano dentro del Estado comienza con la negación de su dignidad, entendiéndola como aquella condición de toda persona como sujeto de derechos y no como un objeto, es decir "cosificándolo" para justificar así cualquier acto de violencia y discriminación en su contra, viendo en él al "*otro*", al "*distinto*" y que eventualmente puede representar un "*enemigo*".

-***Costa Rica como Estado respetuoso del orden convencional emanado del sistema de la Organización de las Naciones Unidas***

Es importante señalar que muchos de los tópicos propuestos ya han sido abordados, regulados e incorporados en el ordenamiento jurídico costarricense.

Costa Rica es suscriptor del Convenio de Europa sobre Ciberdelincuencia (Budapest, 2001) y como tal ha venido adoptando la legislación nacional para hacer frente a las actividades delictivas surgidas con el desarrollo de los avances tecnológicos e informáticos. Incluso en el año 2012 (Leyes N° 9048 y 9135) se incorporó una robusta reforma a nuestro Código Penal, en donde se incluyeron figuras tan diversas como la seducción por medios electrónicos, el daño informático, la estafa informática. Asimismo, como parte del reciente proceso de incorporación a la OCDE, Costa Rica regula ya la responsabilidad penal de las personas jurídicas. Finalmente, Costa Rica reitera su compromiso con la persecución y el juzgamiento de los crímenes más atroces, es decir aquellos que dan sustento normativo y teórico al Derecho Penal Internacional, en el tanto somos parte del Estatuto de Roma y reconocemos la competencia de la Corte Penal Internacional.

A modo de epílogo, el Estado costarricense reitera su voluntad y compromiso con la construcción de una respuesta global, de rango convencional, a los retos que representa la ciberdelincuencia.

Muchas gracias.-