POLITICAS Y ESTRATEGIAS SOBRE DELITOS CIBERNÉTICOS PARA LA COMUNIDAD DEL CARIBE

12-14 June 2019

Santo Domingo, Dominican Republic

SALUDOS:

- Gustavo MONTALVO, Ministro de la Presidencia de Republica Dominicana
- Teniente-Coronel Michael JONES, Director Ejecutivo de la Agencia de seguridad del CARICOM, IMPACS
- Anthony V. TEELUCKSINGH, Presidente del Grupo de Trabajo de la OEA/ REMJA[1] sobre Delitos Cibernéticos
- Manuel ALMEIDA PEREIRA, Jefe de Programa, GLACY+, Oficina de Lucha contra la Ciberdelincuencia del Consejo de Europa

En nombre de la Unión Europea y la Delegación de la UE en la República Dominicana, me complace dar la bienvenida a todos los participantes de la región del Caribe a esta **conferencia de políticas y estrategias sobre delitos cibernéticos**.

Permítanme comenzar expresando nuestro satisfacción por el grupo multisectorial de expertos aquí representados, lo que indica el gran interés en las cuestiones relacionadas con los delitos informáticos y el firme compromiso de las partes interesadas en cooperar en esta área.

La UE se siente honrada de apoyar este proceso, **asociándonos con el Consejo de Europa** en nuestro programa conjunto "Acción global sobre la ciberdelincuencia extendida" GLACY + que desde 2013 ha sido una iniciativa emblemática de desarrollo de capacidades y legislación sobre delitos cibernéticos.

La "**revolución digital**" conlleva una evolución igualmente rápida de comportamientos y patrones criminales, que aprovechan el rápido desarrollo de la tecnología y las lagunas jurídicas existentes. La digitalización ofrece muchas oportunidades de desarrollo para lograr un futuro mejor, pero también viene de la mano con serias vulnerabilidades: no podemos abordar los desafíos de seguridad en el ciberespacio desde un vacío legal.

[1] En 199 se creó en el marco de la OEA, la Reunión de Ministros de Justicia u Otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA),

En esta era digital, hemos sido testigos de que un ciberespacio abierto, global, libre, pacífico y seguro es la base de la prosperidad, el crecimiento y la seguridad de nuestras sociedades. Sin embargo, la **estabilidad cibernética mundial** se basa en la capacidad local y nacional de todos los países para prevenir, reaccionar, investigar y procesar casos de delitos informáticos.

Dado que la cantidad de usuarios de Internet ha aumentado de 1 billón en 2005 a un estimado de 4 billones a principios de 2018, la necesidad de abordar las amenazas planteadas por los delitos cibernéticos es una prioridad clara y debe **atajarse de una manera conjunta**. La responsabilidad recae en todos los actores clave: gobiernos, sector privado, sociedad civil, organizaciones internacionales y regionales, y usuarios finales.

La escala actual, la naturaleza y el impacto del delito cibernético son tales que no solo socavan la confianza en las TIC[2] sino que también representan una grave amenaza para los **derechos fundamentales de las personas**, el estado de derecho en el ciberespacio y las sociedades democráticas.

En 2017, varios incidentes cibernéticos a gran escala, dieron la alarma sobre la necesidad de adoptar medidas concretas para aumentar la resistencia cibernética de los estados así como reforzar la cooperación internacional más estrecha en materia de ciberdelito.

En la Unión Europea, somos conscientes que las medidas coercitivas de aplicación de la ley, como la búsqueda y confiscación de datos, o la interceptación de comunicaciones, representan a menudo interferencias en los derechos de los individuos. Es difícil, a veces, encontrar un equilibrio entre la necesidad de obtener pruebas electrónicas y la necesidad de garantizar los derechos fundamentales y la protección de datos.

En este entorno, las autoridades judiciales y policiales se enfrentan a enormes dificultades para hacer su trabajo de manera efectiva. Los mecanismos tradicionales de aplicación de la ley a menudo se vuelven ineficaces a la luz de las características complejas del delito cibernético. Para **abordar estos desafíos** se necesita:

1. Maximizar el número de países con una legislación interna integral ejecutada por personas debidamente capacitadas.

2. Diseñar nuevas formas de monitorear y reportar la actividad de los delincuentes cibernéticos.

[2] Tecnología, información y comunicación

3. Trabajar juntos a través de las fronteras: construir mecanismos de cooperación y confianza mutua, así como compartir datos e información para investigar y enjuiciar los delitos cibernéticos.

4. Asegurarse de que no existan refugios seguros para los delincuentes y aumentar la capacidad de las autoridades policiales y judiciales para realizar investigaciones, enjuiciamientos y condenas efectivas contra los ciberdelincuentes.

Pero, como ya he mencionado, debemos lograr un equilibrio entre la necesidad de obtener pruebas y la necesidad de garantizar los derechos fundamentales y la protección de datos. Por eso, limitar las nuevas tecnologías no tiene sentido, tenemos que **confiar en los sistemas TIC** para que se fomente el comercio internacional y las comunicaciones.

Lo más importante es que debemos guiarnos por los **principios de necesidad y proporcionalidad** y sobretodo garantizar que los derechos fundamentales y la protección de datos se respeten plenamente en el marco de cualquier solución para mejorar la aplicación del estado de derecho en el ciberespacio y obtener pruebas electrónicas en procedimientos penales.

La **Convención de Budapest** es el intento global de lograr este difícil equilibrio y crear estándares internacionales comunes. Es el acuerdo internacional legalmente vinculante más importante sobre el delito cibernético. La invitación a adherirse a la Convención envía una señal importante sobre la disposición de un país para armonizar sus leyes internas en la lucha seria contra el delito cibernético y participar en la cooperación internacional para este fin.

Según nuestra experiencia, tenemos que trabajar juntos a todos los niveles. Es por este motivo que, paralelamente a los esfuerzos de la UE para abordar la ciberdelincuencia y la ciberseguridad internamente, es **fundamental invertir en la cooperación cibernética internacional.**

Para apoyar este proceso, especialmente en los países en desarrollo de todo el mundo en la lucha contra los delitos informáticos, **la Unión Europea se ha asociado con el Consejo de Europa.**

Una dimensión clave de GLACY + es brindar asistencia personalizada a los países comprometidos con la ejecución de la Convención de Budapest y el fortalecimiento de las capacidades de las instituciones nacionales relevantes en la lucha contra la ciberdelincuencia.

La **necesidad de cooperación a todos los niveles** es un mensaje clave con el que deseo concluir. Me gustaría resaltar el papel fundamental que pueden desempeñar las organizaciones regionales como la Organización de los Estados Americanos y el CARIFORUM.

En los últimos años, la OEA y varios de sus Estados Miembros han estado liderando los esfuerzos de sensibilización sobre el cibercrimen y la ciberseguridad en el hemisferio y desde la UE se lo agradecemos sinceramente.

Además, más cerca de nosotros, CARICOM también ha trabajado para desarrollar su *Plan de Acción de Ciberseguridad y Ciberdelincuencia*. La Unión Europea lanzó en 2018 conjuntamente con IMPACS, un Programa Regional de Ciberdelincuencia para apoyar la ejecución de este Plan de Acción de CARICOM.

Reconocemos que abordar estos problemas de manera holística, por muy técnicos que sean, es muy importante. Necesitamos reformas institucionales, legales y operacionales basadas en estándares internacionales.

Iniciativas como esta conferencia regional son esenciales para identificar las tendencias y necesidades regionales y compartir el conocimiento. Pero para ser eficaz es crucial **llevar de vuelta a sus países y administraciones los mensajes y lecciones aprendidas y asegurar la incorporación en respectivos sistemas nacionales.**

En este sentido, permítanme desearles, en nombre de la Unión Europea, una conferencia muy fructífera y constructiva y reiterarles nuestro compromiso y colaboración en la lucha contra este flagelo que es la ciberdelincuencia.