

image not found or type unknown



www.juventudrebelde.cu

image not found or type unknown



**Los delitos cibernéticos causaron más daños a la economía mundial en 2018 que los de la delincuencia relacionada con las drogas. Autor: Internet Publicado: 10/07/2019 | 09:23 pm**

# **Ciberdelincuencia: un instrumento de injerencia en los asuntos internos de los Estados**

Concluyó en La Habana Foro Internacional por la utilización de las TIC con fines pacíficos

**Publicado: Miércoles 10 julio 2019 | 09:28:53 pm.**

**Publicado por: Airat Jamidulin**

Actualmente el problema del uso de las tecnologías de la información y de las comunicaciones (TIC) con fines criminales es uno de los cinco riesgos globales en la clasificación del Foro Económico Mundial. Si en 2016 los daños a la economía mundial por esa amenaza ascendieron a 445 mil millones de dólares, en 2018, según las estimaciones de las Naciones Unidas, esa cifra se elevó a 1,5 billones. Para este año, se prevé que ascienda a 2,5 billones. Es más que el daño causado por la delincuencia relacionada con las drogas. Esas son solamente las cifras oficiales. En la mayoría de los casos, ni los organismos gubernamentales, ni las empresas privadas, ni los ciudadanos comunes suelen publicar información sobre los delitos cibernéticos cometidos contra ellos. De no adoptarse medidas eficaces, todos los beneficios de la digitalización serán reducidos a la nada y la comunidad mundial correrá un riesgo aún mayor.

Por desgracia, la comunidad internacional en esta área va a la zaga de los malintencionados. La situación se complica por el hecho de que varios países tecnológicamente avanzados, a falta de normas universales, imponen su propia legislación a la comunidad mundial, resuelven los problemas de seguridad por cuenta de otros países, así como recopilan datos –incluso la correspondencia y datos personales– por todo el mundo sin control ninguno y rastrean transacciones financieras.

No resulta sorprendente que los delincuentes empleen cada vez más los mismos programas de servicios especiales y reciban acceso a información valiosa. Cabe citar, por ejemplo, el programa secuestrador WannaCry que infectó ordenadores en más de cien países en 2017 y fue creado sobre la base del software de la Agencia de Seguridad Nacional de los EE. UU. Constituye una grave amenaza no solamente para usuarios comunes de internet, sino también para la comunidad empresarial y élites nacionales que están indefensas ante el robo de dinero de cuentas bancarias y divulgación de información confidencial.

Es evidente que la gama tan amplia del uso indebido de las TIC por delincuentes y estructuras delictivas requiere especializados mecanismos reguladores internacionales que puedan incluir principios y normas generales de la lucha contra esos fenómenos. En el nivel regional, una serie de organizaciones ha elaborado y adoptado los documentos correspondientes.

## **Cooperación, no injerencia**

El primer instrumento de este tipo en la historia ha sido el Acuerdo sobre la Cooperación de Estados miembros de la Comunidad de Estados Independientes (CEI) en la Lucha contra Delitos en la Esfera de Información Computadorizada, que fue firmado en julio de 2001. Ya en aquel entonces Rusia y otros países de la región se preocuparon por la creación de una base jurídica común para desarrollar la cooperación en esa esfera. Eso permitió establecer contactos directos entre organismos encargados del cumplimiento de la ley en una región tan amplia y mejorar el nivel de investigaciones transfronterizas de cibercrimes dentro de la CEI. En 2018, para hacer frente con eficacia a nuevas amenazas, el documento fue sustituido por otro más avanzado: el Acuerdo sobre la Cooperación entre Estados Miembros de la CEI para Luchar contra Delitos en la Esfera de Tecnologías de la Información.

Otro documento regional desarrollado en ese ámbito es el Convenio del Consejo de Europa sobre cibercriminalidad de 2001, más conocido como el Convenio de Budapest. Entre sus objetivos anunciados estaban crear mecanismos para combatir delitos informáticos por armonización de legislaciones nacionales de Estados europeos, desarrollar las prácticas de investigación en el contexto de tales actividades, así como consolidar la cooperación internacional en esa esfera.

Sin embargo, el objetivo verdadero del Convenio de Budapest es diferente. El problema fundamental es la amenaza de la violación de la soberanía estatal y la injerencia en asuntos internos de otros Estados en el proceso de la aplicación de las disposiciones del Convenio de Budapest. En particular, el apartado b) del artículo 32 del Convenio permite a los Estados partes recibir acceso transfronterizo a la información cuya fuente se encuentra en otro Estado, no solamente sin autorización alguna, sino también sin notificar a los órganos competentes de ese Estado. Eso deja grandes oportunidades a Estados tecnológicamente adelantados para infiltrarse libremente y de forma legal en el espacio informativo de otros que son parte del Convenio de Budapest, que generalmente no saben de eso. Es claro que ese enfoque viola derechos y libertades humanos fundamentales, en particular, el derecho a la privacidad.

Otro punto clave. Todos sabemos que el terrorismo es una forma de delincuencia, y los vínculos entre los piratas informáticos y organizaciones terroristas siguen creciendo. Pero el Convenio de Budapest no es aplicable para luchar contra acciones terroristas en internet.

Además, el Convenio penaliza solamente nueve categorías de delitos. Hoy en día, hay más de 30 delitos principales y una gran multitud de variantes secundarias y conexas. Es porque el documento fue preparado y adoptado en los decenios de 1990 y 2000, cuando el nivel de desarrollo de las TIC era bastante bajo. En el momento de su adopción muchos tipos de amenazas en la red presentes ahora, simplemente eran desconocidas.

Por eso no resulta sorprendente que el Convenio de Budapest no se use en los tribunales como base jurídica. Ese documento fue desarrollado para otros fines.

Bajo el pretexto de la lucha contra ciberdelincuentes, los servicios especiales de Estados tecnológicamente adelantados llevan a cabo operaciones encubiertas en el espacio de la información de otros países, incluso para lograr sus objetivos políticos, que pueden incluir recopilación incontrolada de datos personales y coerción para lograr la cooperación de organismos nacionales encargados del cumplimiento de la ley con el fin de lograr los objetivos de la política exterior. Los fundadores del Convenio de Budapest instan muy activamente a representantes de países en desarrollo a que se adhieran a su instrumento. Hacen hincapié en la «ayuda técnica», que de hecho refuerza la «brecha digital» entre Estados desarrollados y en desarrollo, educan a personal técnico obediente a ellos, que hace a esos países muy vulnerables desde el punto de vista político.

## **Un instrumento jurídico internacional contra los ciberdelitos**

Hoy en día la consecuencia de un gran número de convenios regionales ha sido la fragmentación de posiciones a nivel internacional, que impide la elaboración de un entendimiento común de los aspectos claves para contrarrestar las actividades ilegales en la esfera de la información.

Es importante destacar que la ciberdelincuencia es un fenómeno transnacional y es muy probable que malhechores que se encuentren en el territorio de un Estado pueden cometer delitos con el uso de las TIC contra otro Estado en que no se aplica uno u otro documento regional. En ese contexto resulta evidente que es necesario desarrollar un mecanismo jurídico internacional universal en esa esfera. Un instrumento así podría ser un convenio preparado bajo los auspicios de las Naciones Unidas para la lucha contra delitos en el uso de las TIC que tome en cuenta las realidades de todos los países sin excepción y se base en los principios de igualdad soberana de las partes y la no injerencia en los asuntos internos de los Estados. La idea de elaborar un documento de ese tipo figuró por la primera vez en la declaración final del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (Brasil, 2010).

A ese respecto, Rusia ha elaborado y presentado un proyecto correspondiente de un convenio universal sobre la cooperación en la lucha contra la delincuencia informática que vemos como un documento de reflexión y puede servir de base para la elaboración del primer acuerdo global en esa esfera. Ha sido presentado más de una vez en varias importantes plataformas especializadas, y el 28 de diciembre de 2017 se convirtió en un documento oficial del 72º período de sesiones de la Asamblea General de las Naciones Unidas.

El proyecto de ese convenio se considera como un instrumento multilateral jurídico internacional que refleja la naturaleza de delitos en el uso de las TIC y cuyo objetivo es luchar contra esos delitos. Durante su elaboración se tomaron en cuenta en particular las disposiciones de la Convención de las Naciones Unidas contra la

Corrupción, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y algunos convenios globales antiterroristas.

El proyecto ruso es en gran medida innovador. Estipula el establecimiento de la jurisdicción universal, un amplio mecanismo conceptual, ayuda técnica, términos de asistencia jurídica mutua en la etapa previa al juicio, incluso en los casos de emergencia, y un mecanismo eficaz para poner en práctica las disposiciones del Convenio.

En cuanto a los individuos sospechosos de delitos y cuya extradición ha sido solicitada, el Convenio establece el principio de que no haya impunidad, de «extraditar o enjuiciar», uno de los principios fundamentales de la cooperación jurídica penal internacional. El Convenio establece la oportunidad de una participación confortable para todos los Estados sin daño al desarrollo del Derecho Internacional y se basa en los principios de igualdad soberana y no injerencia en los asuntos internos de los Estados. El documento fue desarrollado con la participación tanto de los expertos gubernamentales como de los representantes de empresas de la tecnología de la información. Es decir, el proyecto del convenio fue desarrollado por profesionales para los mismos profesionales y los que quieren llegar a ser profesionales.

Es notable que los fundadores del Convenio de Budapest han visto en ese proyecto una amenaza a su instrumento, que no fue elaborado bajo los auspicios de las Naciones Unidas y de hecho no se corresponde con sus principios fundamentales —la no injerencia en los asuntos internos de otros Estados y la igualdad soberana de las partes—. Por eso recurrieron a las tácticas de la preservación del equilibrio corriente, lo que significa que en el marco de la única plataforma activa de las Naciones Unidas bloquean la creación de un convenio universal, mientras que otros países en ausencia de un marco jurídico eficaz y por desesperanza elaboran su propia legislación o se adhieren al Convenio del Consejo de Europa. Son evidentes las diferencias conceptuales que han conducido a la comunidad mundial a un callejón sin salida y han dado vía libre a los delincuentes.

## **Rusia y la búsqueda de consenso en la comunidad internacional**

En tales condiciones, Rusia no tiene la intención de esperar a la exacerbación del daño causado por ciberdelincuentes y quedarse de brazos cruzados. En 2018 preparamos el proyecto de la primera resolución de la Asamblea General de las Naciones Unidas en la historia sobre la lucha contra el uso de las TIC con fines criminales.

Su parte dispositiva presupone la inclusión de un tema separado a la agenda preliminar del 74° período de sesiones de la Asamblea General de las Naciones Unidas sobre ese asunto (La lucha contra el uso de las TIC con fines criminales) y la preparación por el Secretario General de las Naciones sobre la base de los datos proporcionados por los Estados miembros de las Naciones Unidas de un reporte sobre el asunto, que será examinado durante el 74° período de sesiones de la Asamblea General de las Naciones Unidas. En diciembre de 2018 esa resolución fue aprobada por mayoría en la Asamblea General de las Naciones Unidas. La apoyó la mayoría absoluta de países en desarrollo de Asia, África, América Latina, e incluso muchos países partes del Convenio de Budapest. Se opusieron la UE, los EE. UU. y sus aliados más próximos, que no quieren dejar a otros actores acercarse a ese asunto estratégico.

Ahora la comunidad mundial tiene la oportunidad de realizar un debate en el marco del 74° período de sesiones de la Asamblea General, el primer debate sobre modos de encontrar un consenso acerca del desarrollo futuro de la cooperación en esa esfera y la elaboración de un plan de acción para salir de ese estancamiento. Es evidente que una forma de resolver esos problemas será la idea de que conviene establecer principios y normas

universales que sean compartidos por todas las partes interesadas y que sienten las bases para una cooperación internacional efectiva en esa esfera.

**Airat Jamidulin (Airat Jamidulin es asistente del Representante Especial del Presidente de la Federación de Rusia para la cooperación internacional en el campo de la seguridad de la información Andréi Krutskij)**

<http://www.juventudrebelde.cu/ciencia-tecnica/2019-07-10/ciberdelincuencia-un-instrumento-de-injerencia-en-los-asuntos-internos-de-los-estados>

**Juventud Rebelde** | Diario de la juventud cubana  
Copyright © 2017 Juventud Rebelde