Manifiesto Multilateral

Priorizar los intereses de las personas en el futuro convenio de la ONU sobre la ciberdelincuencia

El mundo está siendo testigo de una rápida evolución de las amenazas cibernéticas viéndose nuestra seguridad colectiva comprometida por una, cada vez mayor, frecuencia, sofisticación e intensidad de los ataques. Los delitos cibernéticos suponen nuevos riesgos para la seguridad, la dignidad y la equidad de las personas, y se convierten en desafíos transfronterizos que ningún actor individual puede afrontar en solitario. Por ello, resulta esencial adoptar un enfoque multilateral para combatir el uso malintencionado de las tecnologías de la información y las comunicaciones (TIC) y para proteger y prevenir a los usuarios de dichas tecnologías.

Asimismo, estamos siguiendo de cerca el proceso de negociación del futuro convenio sobre la ciberdelincuencia, establecido por la resolución 74/247 de la Asamblea General de las Naciones Unidas. Dados los instrumentos internacionales y regionales existentes para combatir el ciberdelito, instamos a la comunidad internacional a evitar la duplicación de esfuerzos y a centrarse en aquellos que refuercen la aplicación de los marcos establecidos.

En este contexto, y reconociendo el voto mayoritario en las Naciones Unidas, enunciamos un conjunto de principios que, a nuestro juicio, deberían seguir los participantes en el proceso para consolidar los derechos y libertades necesarios que permitan lograr un ciberespacio libre, abierto, seguro y pacífico, y que refuercen el respeto por el estado de derecho en el ciberespacio.

Proteger a las víctimas

El nuevo instrumento internacional de lucha contra la ciberdelincuencia debería tener como principales objetivos la protección de los destinatarios y víctimas, y la disponibilidad de soluciones eficaces que se basen en un marco de protección de los derechos humanos. Durante mucho tiempo, múltiples gobiernos se han escudado en la lucha contra la ciberdelincuencia para ampliar el control estatal a través de medidas legislativas, tales como ilegalizar la publicación y difusión de información que les incomodase, imponer una vigilancia generalizada y restringir la privacidad de sus ciudadanos en nombre de la lucha contra el terrorismo. Por ello, el nuevo convenio debería garantizar la protección de la seguridad, la equidad y la dignidad humanas, en consonancia con las obligaciones de cualquier Estado para con sus ciudadanos. Para proteger a las víctimas, un futuro instrumento jurídico debería garantizar que la calificación de un comportamiento como delictivo se apoye en un alcance adaptable, aunque estrecho, a fin de

prevenir la criminalización de aquellas conductas que no sean sino el ejercicio de libertades fundamentales y derechos humanos.

Combatir con eficacia la ciberdelincuencia mediante el fortalecimiento de la cooperación internacional

El objetivo principal de cualquier nuevo convenio de la ONU sobre ciberdelincuencia debería ser combatirla a la vez que se da prioridad a los intereses de las personas. El acuerdo debería tener como piedra angular la defensa de los derechos humanos y la eficaz puesta en marcha de las soluciones existentes para fortalecer la cooperación internacional entre diferentes autoridades judiciales y cuerpos de seguridad, en el marco de un control transparente. Este debería, igualmente, destacar la necesidad de reforzar dicha colaboración internacional e intersectorial y de armonizar los marcos existentes para la investigación y el procesamiento judicial de los delitos cibernéticos.

Mantener intactas las obligaciones internacionales existentes

Un nuevo convenio sobre ciberdelincuencia no puede abrir la puerta a que los Estados reduzcan sus obligaciones vigentes en materia de legislación internacional, especialmente en lo relativa a derechos humanos. En esta línea, un nuevo acuerdo no debe reemplazar, sino complementar o simplificar, las obligaciones que los Estados han contraído entre sí. Debería reforzar las obligaciones impuestas por el derecho internacional y destacar su impacto positivo.

Reforzar los mecanismos de rendición de cuentas

Cualquier nuevo convenio debería centrarse en una rendición de cuentas basada en pruebas, de forma que se facilitase a los afectados por un ciberdelito la posibilidad de recurrir judicialmente y de buscar algún tipo de reparación. Los Estados necesitan reducir el espacio de acción de los delincuentes, no sólo mediante la puesta en marcha de los marcos legales internacionales acordados y trabajando de forma conjunta en los procesamientos judiciales, sino incentivando los consorcios público-privados para combatir la ciberdelincuencia. Debería tenerse en cuenta el impacto de aquella en el conjunto de la sociedad cuando se responsabiliza a quien ha cometido el daño.

Mantener la atemporalidad de los convenios

Dado que la ciberdelincuencia evoluciona de forma rápida y constante, las definiciones sobre esta probablemente deberán evolucionar a la vez, siendo el alcance de cualquier convenio definido de forma clara y sin ninguna referencia a tecnologías específicas.

Preservar la apertura de Internet

Un mayor número cada vez mayor de países persigue el objetivo de dividir Internet en diversas esferas nacionales de influencia y control. La firma de un nuevo convenio sobre ciberdelincuencia no ha de servir como justificación, ni excusa, para que regímenes no

democráticos amenacen aún más la Internet abierta, al cerrar sus fronteras digitales al resto del mundo en nombre de la prevención de ciberdelitos. Para preservar una Internet abierta, el nuevo acuerdo debería garantizar que es alcanzado para fijar reglas jurisdiccionales que tengan en cuenta la realidad de la Internet globalizada y el libre flujo de información.

ESTABLECER LOS PROCESOS ADECUADOS

Aplicar, en todo momento, un enfoque que incluya a todos los interesados

A lo largo de todo el proceso [de negociación del nuevo convenio], debería haber una permanente consulta a, y una significativa participación de, las diferentes partes interesadas. Deben incluirse y considerarse los intereses de la sociedad civil, el sector empresarial, el ámbito académico, los investigadores, los expertos en tecnología y las instituciones científicas y de investigación. Para lograr el equilibrio adecuado durante la negociación, es necesario que se consulte a expertos en ciberseguridad, en gobernanza de Internet, en derecho internacional y en derechos humanos, entre otros temas.

Promover la transparencia

Las negociaciones sobre el futuro convenio deberían ser lo más transparentes posible. Las organizaciones, los individuos y los Estados cuyos intereses y derechos puedan verse afectados por las negociaciones deberían tener la oportunidad de responder y ser escuchados. El calendario de, y los participantes en, las sesiones de negociación deberían, por ejemplo, ponerse a disposición del público, así como debería estarlo también cualquier borrador del texto en elaboración.

Clarificar el alcance

Una definición demasiado amplia del término 'ciberdelincuencia' tiene el potencial de criminalizar un gran conjunto de actividades que vayan mas lejos del verdadero delito. Los participantes en la negociación del futuro texto deberían mostrarse prudentes a la hora de definir el alcance de los principales delitos que pretendan castigar, a fin de garantizar que el nuevo convenio no pueda ser empleado para justificar la represión contra la oposición política, los defensores de los derechos humanos o la sociedad civil.

Adoptar un enfoque basado en el consenso

Cualquier nuevo convenio sobre ciberdelincuencia debería ser fruto del consenso e incluir disposiciones acordadas por distintos países y regiones, siendo el resultado de un intenso proceso de consulta a expertos y a los pertinentes grupos de interés.

Por favor, visite la página web de CyberPeace Institute o de Cybersecurity Tech Accord para ver la lista de signatarios actualizada. Para más información, por favor póngase en contacto a través de info@cyberpeaceinstitute.org o info@cybertechaccord.org.