Carta abierta a la Asamblea General de Naciones Unidas: La propuesta de convención internacional sobre ciberdelitos constituye una amenaza para los derechos humanos

Sus Excelencias:

La lucha contra el ciberdelito es un desafío clave que requiere cooperación internacional. Sin embargo, el marco adoptado para la resolución preliminar “Combatir el uso de tecnologías de la información y la comunicación con fines delictivos”(A/C.3/74/L.11/Rev.1) en el Tercer Comité de la Asamblea General de Naciones Unidas (UNGA) contiene errores fundamentales y puede terminar restringiendo el uso de internet para la protección de los derechos humanos, así como para el desarrollo social y económico. Las organizaciones abajo firmantes instamos a su delegación a votar en contra del documento preliminar de la resolución.

La resolución “establece un comité intergubernamental abierto ad hoc de expertos, representantes de todas las regiones, con el objetivo de elaborar una convención internacional amplia para combatir el uso de tecnologías de la información y la comunicación con fines delictivos”. No estamos convencidos/as de que sea necesario contar con una nueva convención internacional sobre ciberdelincuencia. Nos preocupa gravemente que el marco propuesto en la “Convención preliminar de Naciones Unidas sobre cooperación para combatir la ciberdelincuencia” (A/C.3/72/12) para el trabajo de Naciones Unidas en esta área que fue puesto en circulación por la Federación Rusa limite el uso de internet para el ejercicio de los derechos humanos, así como para la promoción del desarrollo social y económico.

Nuestra inquietud relativa a la resolución y el proceso que se iniciaría a partir de la misma se basa en los siguientes puntos:

Primero, en la resolución no se define claramente qué es el “uso de tecnologías de información y comunicación con fines delictivos”. El texto incluye tanto asuntos de ciberseguridad (delitos que causan un impacto en la “estabilidad de infraestructura clave de Estados y empresas”), como acciones delictivas posibilitadas por las TIC (por ejemplo, “los traficantes de personas [...] pueden aprovechar las tecnologías de

información y comunicación para llevar a cabo actividades delictivas y criminales"). La ausencia de especificidad no sólo es preocupante porque no es adecuada, sino que, al no definir la expresión, acaba por fomentar la posibilidad de que cualquier conducta normal en línea se considere un delito, aunque esté protegida por la legislación internacional sobre derechos humanos.

Segundo, la tipificación de actividades comunes en línea por parte de individuos y organizaciones como delitos mediante la aplicación de leyes contra la ciberdelincuencia constituye una tendencia creciente en muchos países del mundo. El Relator Especial de Naciones Unidas sobre el derecho a la libertad y el de reunión y asociación pacífica observa que: "La oleada de leyes y políticas que apuntan a combatir la ciberdelincuencia ha abierto la puerta al castigo y vigilancia de activistas y manifestantes en muchos países del mundo".[1] Como se señala en el informe, dichas leyes se utilizan para condenar el acceso y uso de comunicaciones digitales seguras (mediante el uso de cifrado, por ejemplo) que son fundamentales para el trabajo de la sociedad civil, los y las activistas por los derechos humanos y los colectivos de periodistas, así como para instituciones públicas y privadas que dependen de una conexión estable y segura a internet; condenar formatos legítimos de expresión, asociación y asamblea en línea mediante el uso de términos vagos e indefinidos que se pueden aplicar de manera arbitraria o discrecional y producen incertidumbre legal; y para darle un poder más amplio a los gobiernos a fin de que puedan bloquear sitios web que las autoridades consideren peligrosos, o incluso para bloquear redes, aplicaciones y servicios enteros que facilitan el acceso e intercambio de información en línea.

Si bien la legislación sobre ciberdelitos puede ser necesaria y reforzar a las instituciones democráticas, en caso de ser mal utilizada puede tener un efecto paralizante y acabar por impedir que la gente use internet para ejercer sus derechos tanto en línea como fuera de línea. Como se le ha planteado ya a varios gobiernos a raíz de numerosos Procedimientos Especiales de Naciones Unidas, la legislación contra ciberdelitos puede terminar provocando arrestos, detenciones e incluso muertes de forma arbitraria.[2] La referencia a los derechos humanos que se incluye en la

1 Informe 2019 del Relator Especial sobre el derecho a la libre asociación y asamblea pacífica (A/HRC/41/4)

2 Arabia Saudita (SAU 13/2014) La Comunicación de los/as Relatores/as Especiales sobre la promoción y protección del derecho a la libertad de opinión y de expresión; libertad de religión o de credo; y sobre la situación de los/as activistas en defensa de los derechos humanos en relación a la sentencia del Sr. Raef Badawi por el cargo de "insulto al Islam" según la Ley contra la ciberdelincuencia; la Comunicación del Grupo de trabajo sobre detenciones arbitrarias de Bangladesh (BGD 14/2013) y las de los Relatores/as Especiales sobre la promoción y protección del derecho a la libertad de opinión y expresión; los derechos a la reunión pacífica y a la asociación; y sobre la situación de los/as activistas en defensa de los derechos humanos acerca de la situación del Sr. Nasiruddin Elan, director de Odhikar, una organización

resolución preliminar, que se limita a reafirmar la importancia del respeto hacia los derechos humanos y las libertades fundamentales en el uso de TIC, es insuficiente para la salvaguarda de los derechos humanos en lo que se refiere a ciberdelitos.

Tercero, el "Proyecto de Convención de Naciones Unidas para la Cooperación en la lucha contra Ciberdelitos", cuyo objetivo es servir de base para el desarrollo de una convención internacional amplia, provoca varias inquietudes. Es de particular importancia el hecho de que dicha Convención proponga ir mucho más lejos de lo permitido en el Convenio de Budapest en relación al acceso transfronterizo de datos, incluso en cuanto que no permite que los países firmantes se nieguen a brindar acceso a los datos requeridos.[3] El Proyecto de Convención acabaría por establecer a la ONU como punto de aplicación de la legislación creando una Comisión Técnica Internacional para el Combate contra la delincuencia en TIC, entre otros mecanismos de ejecución de la ley. Varias cláusulas del Proyecto de Convención reflejan las del Convenio de Budapest. Sin embargo, no se hace referencia al equilibrio que debe existir entre la implementación de las leyes y el respeto por los derechos humanos fundamentales, y tampoco hay referencias al principio de proporcionalidad y el derecho a un juicio justo. Dado que la Federación Rusa ha hecho un gran esfuerzo para ampliar el control del gobierno sobre internet y aprobó al principio de este mes una ley que se conoce como "la soberanía de internet",[4] es esencial analizar detalladamente y seguir de cerca su rol de liderazgo en el desarrollo de un acuerdo internacional vinculante sobre la ciberdelincuencia.

no gubernamental, que fue arrestado por violar supuestamente la Sección 57 de la Ley sobre Tecnologías de la Información y Comunicación y presentado ante el Tribunal de Ciberdelitos; UAE (ARE 5/2013) Comunicación de los/as Relatores/as Especiales sobre la promoción y la protección del derecho a la libertad de opinión y expresión; los derechos de asamblea pacífica y asociación; sobre la situación de los/as defensores/as de los derechos humanos; y sobre la tortura y otros tratos o castigos inhumanos y degradantes en el supuesto uso de una nueva Ley sobre ciberedelincuencia que impone restricciones indebidas a la libertad de expresión en línea;la Comunicación de la Relatoría Especial de Iran (IRN 27/2012) sobre la promoción y protección del derecho a la libertad de opinión y expresión; la Relatoría Especial sobre los/as defensores/as de los derechos humanos; Relatoría Especial sobre la situación de los derechos humanos en la República Islámica de Irán; la Relatoría Especial sobre ejecuciones extrajudiciales, sumarias, o arbitrarias, y sobre la tortura y otros tratos o castigos crueles, inhumanos, o degradantes sobre la tortura que supuestamente provocó la muerte de Sattar Beheshti mientras estaba bajo custodia, luego de estar bajo arresto con cargos de ciberdelincuencia.

3 Articles 51-56 of the Draft Convention establish conditions for the availability of data from other states. While they do not go so far as to say that all states would be forced to turn over all relevant information, these articles put a strong degree of pressure to do so on all signatories by requiring that domestic law be modified to support turnover of traffic and content data under the conditions defined in the convention and the licences agreed upon by the states.

4 https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online

Cuarto, no creemos que sea necesaria una nueva convención internacional sobre ciberdelitos. Sería mejor dedicarse a mejorar los instrumentos existentes, en lugar de destinar los escasos recursos que hay para crear un nuevo marco internacional, lo que además seguramente llevará años y es muy poco probable que se alcance un consenso. Ya hay otras secciones de Naciones Unidas dedicadas a trabajar con ciberdelitos, específicamente la Oficina de Drogas y Delitos de Naciones Unidas (UNODC), además de las iniciativas que existen a nivel nacional y regional. Según la base de datos de UNODC sobre legislación relativa a ciberdelincuencia, más de 180 países cuentan con legislación sustantiva y procedimental en relación a la ciberdelincuencia y la evidencia electrónica.[5] Sin duda, existen desafíos en cuanto a la fuerza que tienen las leyes nacionales, además de la capacidad de los gobiernos para implementarlas; sin embargo, ya hay un proceso de la ONU que trabaja para tratar estos asuntos. El Grupo intergubernamental abierto de expertos de la ONU para la realización de un estudio amplio sobre la ciberdelincuencia presentará su informe en 2021. Dicho informe deberá incluir sus hallazgos y recomendaciones sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional.[6] Existe en la actualidad un proceso en marcha para desarrollar el Protocolo Adicional al Convenio de Budapest, que es el instrumento con mayor ratificación internacional que existe en relación a la ciberdelincuencia.[7]

Por último, combatir la ciberdelincuencia es una tarea necesariamente multisectorial. Se requiere la participación de funcionarios y expertos gubernamentales, miembros de la comunidad técnica, la sociedad civil, el sector privado y las instituciones científicas y de investigación. La creación de un comité intergubernamental ad hoc de expertos para tratar sobre ciberdelitos excluiría a sectores claves que podrían aportar conocimiento y perspectivas de mucho valor tanto para el combate efectivo del uso de las TIC con fines delictivos, como para garantizar que dicho esfuerzo no anule la posibilidad de aprovechar las TIC para ejercer los derechos humanos y promover el desarrollo social y económico.

Instamos a su delegación a votar contra la resolución A/C.3/74/L/11/Rev.1 que trata sobre "Combatir el uso de tecnologías de la información y la comunicación

5 La base de datos contiene extractos de las leyes relevantes a situaciones de ciberdelincuencia y asuntos transversales, y habilita el acceso de los/as usuarios/as a todos los documentos de la legislación.
6 https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2019.html
7 La sociedad civil está comprometida en el desarrollo del Segundo Protocolo Adicional al Convenio de Budapest con el fin de superar algunas faltas de la Convención, en particular, para garantizar que las solicitudes de datos personales entre países respeten los derechos humanos. https://www.eff.org/document/joint-civil-society-response-discussion-guide-2nd-additional-protocol-budapest-convention

con fines delictivos" y a trabajar a fin de garantizar que las iniciativas relativas a la ciberdelincuencia incluyan a todas las partes interesadas.

Atentamente,

7amleh - The Arab Center for the Advancement of Social Media
Access Now
Africa Freedom of Information Centre
Albanian Media Institute
Americans for Democracy & Human Rights in Bahrain
ARTICLE 19
Association for Progressive Communications (APC)
Bangladesh NGOs Network for Radio and Communication
BlueLink – Bulgaria
Bytes for All (B4A) – Pakistán
Child Rights International Network (CRIN)
Derechos Digitales – América Latina
Digital Rights Foundation
Electronic Frontier Foundation (EFF)
eQuality Project, University of Ottawa – Canadá
Fundación Huaira – Quito, Ecuador
Fundación Internet Bolivia
Global Partners Digital
Hiperderecho – Perú
Human Rights in China
Internet Governance Project
Internet Policy Observatory – Pakistán
Internet Society
IPANDETEC – América Central
Jonction – Senegal
Media Institute of Southern Africa (MISA)
Media Matters for Democracy – Pakistán
Paradigm Initiative – Nigeria
Privacy International
Red en Defensa de los Derechos Digitales (R3D)
Research ICT Africa
Software Freedom Law Center
TEDIC – Paraguay
Usuarios Digitales
Vigilance for Democracy and the Civic State – Túnez
YMCA Computer Training Centre and Digital Studio – Gambia

Individuos:

(Lista de afiliaciones para su identificación)

Dr. Jennifer Barrigar
Canadá

Tamir Israel
Abogado, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Douwe Korff
Profesor Emérito de Derecho Internacional, Universidad Metropolitana de Londres, y Profesor Asociado de Oxford Martin School, Universidad de Oxford

Joy Liddicoat
Investigadora, Universidad de Otago, Nueva Zelanda, y vicepresidenta de InternetNZ

Damian Loreti
Universidad de Buenos Aires, Argentina

Valerie Steeves
Profesora, Departamento de Criminología, Universidad de Ottawa, Canadá