

## Contribución conjunta de Derechos Digitales, R3D, IPANDETEC e Hiperderecho para el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos - Sexto período de sesiones

### Resumen ejecutivo

Las organizaciones **Derechos Digitales**, **Red en Defensa de los Derechos Digitales (R3D)**, e **Instituto Panamericano de Derecho y Tecnologías (IPANDETEC)** e **Hiperderecho**, pertenecientes al consorcio AlSur<sup>1</sup> de 11 organizaciones de la sociedad civil y el ámbito académico que buscan fortalecer los derechos humanos en entorno digitales, presentan sus propuestas con respecto al Proyecto de texto del Comité Especial encargado de elaborar una Convención internacional general sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos ([A/AC.291/22](#)).

Nuestras recomendaciones se resumen en los siguientes puntos:

#### a) **Perspectiva de género.**

Los espacios digitales se insertan en sociedades afectadas por desigualdades estructurales preexistentes las cuales pueden ser agravadas y perpetuadas por leyes y normas. Por ende, se recomienda que la referencia de perspectiva de género vaya más allá del Preámbulo del documento y se incorpore de manera transversal a toda la Convención y en cada uno de sus artículos. Más específicamente, se recomienda introducir los siguientes cambios: en los **Artículos 24 y 36**, se puede incluir la referencia a “necesidad de aplicar la perspectiva de género”. A su vez, en el **Artículo 40**, tener disposiciones que especifiquen que los Estados tienen la posibilidad de denegar la solicitud de asistencia judicial si existen serias dudas de que la solicitud pueda basarse en una discriminación por razón de sexo u orientación sexual. En el **Artículo 54**, reincorporar la necesidad de incorporar métodos para integrar la perspectiva de género en la elaboración de políticas, la legislación y la programación.

#### b) **Criminalización.**

Celebramos la reducción del catálogo de delitos de 30 a 11 delitos, centrándose así en aquello que se cometen a través y contra sistemas informáticos. Sin embargo, persisten ambigüedades que pueden criminalizar actividades periodísticas, de defensa de derechos humanos y de investigación en seguridad digital. Al ser América Latina una región que registra un uso arbitrario de tecnologías de vigilancia y mecanismos de persecución judicial contra estos grupos, es aún más necesario evitar brindar mecanismos que refuercen esta situación.

En ese sentido, recomendamos que en el **Capítulo II sobre criminalización**, en los **Artículos 6, 8 y 9** se sustituya el término “intención deshonesto” por “intención dolosa” para reducir el margen de interpretación. Es necesario **evaluar la permanencia del Artículo 10** debido a que éste repite delitos ya mencionados en

<sup>1</sup> Ver: <https://www.alsur.lat/>

los Artículos 6 al 9. Otro punto importante en este apartado se refiere a considerar los impactos de género de la criminalización sobre la base de que la libertad de expresión es esencial para la igualdad de género. Las legislaciones que criminalizan la capacidad de expresar demandas sociales relacionadas con desigualdades estructurales de género atentan directamente contra su visibilización y manifestación.

También se sugiere **establecer una excepción legítima en el Artículo 15** sobre difusión de material íntimo para fines de obtención de evidencia y asesoría legal, pues al no tenerla se abre la puerta a revictimización y criminalización de las propias víctimas. Es importante que el texto elimine la intencionalidad de causar un daño como requisito necesario para este delito y lo sustituya por “a sabiendas de la falta de consentimiento de la víctima”.

Se menciona también que el documento analizado incluye un nuevo Artículo (Art. 17) el cual abre una brecha para criminalizar y perseguir acciones calificadas como delitos en tratados y protocolos internacionales cuando se cometan mediante el uso de tecnologías. Esto es ambiguo y supone una grave afectación a la soberanía de los países y a los derechos humanos. La amplitud permite que se puedan reincorporar aquellos delitos de contenido que ya fueron eliminados de anteriores versiones del Convenio, por lo cual **recomendamos eliminar el Artículo 17 en su totalidad.**

#### c) **Medidas procesales y aplicación de la ley**

En relación a las medidas procesales incluidas en el documento, observamos varios artículos. Recomendamos eliminar los incisos b y c del **Artículo 23**, pues estos habilitan a que la Convención sea aplicada a otros delitos penales no comprendidos en el propio documento y que fuerzas del orden interfieran en el derecho a la libertad de expresión arguyendo la investigación de delitos menores.

Por otra parte, el **Artículo 24** introduce facultades de vigilancia muy intrusivas, por lo que es necesario agregar un primer párrafo que establezca principios de legalidad, proporcionalidad y necesidad, así como la obligación de proteger de forma adecuada los derechos humanos y las libertades.

En los **Artículos 29 y 30**, bajo los mismos argumentos referentes a la necesidad de limitar el alcance de la Convención para evitar que ésta sea utilizada de manera abusiva o arbitraria, proponemos incluir la referencia de que dichos artículos serán aplicados únicamente a los delitos incluidos en los artículos 6 a 16 de la Convención.

#### d) **Cooperación internacional.**

En el Capítulo V notamos la falta de salvaguardas en las facultades de asistencia legal y técnica mutua que se le dan a los Estados. Es necesario agregar el requisito de doble criminalidad en el **Artículo 35** para poder llevar adelante la cooperación internacional, lo cual asegura que ésta no sea solicitada por motivos políticos, discriminación basada en género u otros de tipo arbitrario. Por otra parte, el **Artículo 36** solamente menciona el derecho interno aplicable en materia de protección de datos personales como excepción para transmitir estos, lo cual es insuficiente pues el derecho a la protección de datos personales es reconocido internacionalmente y además perjudicaría a ciudadanos de países donde la legislación en esta materia no está vigente. Los Estados partes no deberían estar obligados a transmitir datos personales si no se cumplen los principios de tratamiento lícito y justo,



transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad.

Finalmente, se sugiere que este Capítulo aplique una perspectiva de género al tomar en cuenta impactos diferenciados con respecto a la recopilación de datos para las comunidades en situación de vulnerabilidad o de alto riesgo. Es crucial que la recopilación, almacenamiento y transferencia de datos esté sujeto a un análisis interseccional de género para identificar los riesgos para la seguridad individual que dichos procedimientos conllevan.