FES BRIEFING

¿QUÉ ES EL TRATADO DE LA ORGANIZACIÓN DE LAS NACIONES UNIDAS SOBRE EL CIBERCRIMEN Y POR QUÉ ES IMPORTANTE?*

Isabella Wilkinson**

Octubre de 2023

FRIEDRICH EBERT STIFTUNG
RED DE SEGURIDAD INCLUYENTE

1. ¿QUÉ ES EL TRATADO DE LA ONU SOBRE EL CIBERCRIMEN?

Desde mayo de 2021, los Estados miembros de la ONU han venido negociando un tratado internacional para combatir el cibercrimen. De ser adoptado por la Asamblea General, sería el primer instrumento vinculante de las Naciones Unidas en la materia. El tratado podría convertirse en un importante marco jurídico de alcance global para la cooperación internacional en materia de prevención e investigación del cibercrimen y para procesar penalmente a los cibercriminales.

Pero si el tratado carece de un ámbito de aplicación claramente definido y de las garantías suficientes, podría poner en peligro los derechos humanos –tanto dentro como fuera de Internet– y los gobiernos represivos podrían abusar de sus disposiciones para criminalizar la libertad de expresión en Internet. Podría amenazar también los derechos digitales al legitimar las investigaciones intrusivas y el acceso sin restricciones a la información personal por parte de los organismos encargados de velar por el cumplimiento de la ley.

* Este artículo se publicó originalmente en inglés en la página web de Chatham House: https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter

** Investigadora asociada del Programa de Seguridad Internacional de Chatham House.
Traducción del inglés por Yenni Castro, Valestra Editorial.

2. ¿QUÉ ES EL CIBERCRIMEN?

No existe una definición de cibercrimen aceptada universalmente. Un enfoque común consiste en definirla en dos categorías: delitos que dependen del entorno cibernético [*cyber-dependent crimes*] y delitos que son facilitados por el entorno cibernético [*cyber-enabled crimes*].

Los delitos que dependen del entorno cibernético son aquellos que solo pueden cometerse mediante el uso de las tecnologías de la información y la comunicación (TIC). Un ejemplo notorio es el *ransomware*: hackear el dispositivo de una organización o individuo, encriptar los datos y exigir un pago por desencriptarlos.

"Si el tratado carece de un ámbito de aplicación claramente definido y de las garantías suficientes, podría poner en peligro los derechos humanos –tanto dentro como fuera de Internet– y los gobiernos represivos podrían abusar de sus disposiciones para criminalizar la libertad de expresión en Internet".

Los delitos que son facilitados por el entorno cibernético son los mismos delitos tradicionales, pero se han transformado en su velocidad, escala y alcance mediante el uso de las tecnologías de la información y la comunicación, como las estafas bancarias en Internet, el robo o fraude de identidad y la explotación sexual infantil en Internet.

3. ¿POR QUÉ ES IMPORTANTE UN NUEVO TRATADO SOBRE CIBERCRIMEN?

En los últimos veinte años, las nuevas tecnologías y los actores que generan amenazas han evolucionado a un ritmo sin precedentes. Asimismo, se han multiplicado los esfuerzos nacionales e internacionales para luchar contra el uso delictivo de las TIC.

Las víctimas del cibercrimen van desde individuos y comunidades hasta empresas y gobiernos enteros. Las estafas, el fraude, la extorsión y el acoso cibernéticos van en aumento. Se calcula que, tan solo en los últimos cinco años, las estafas románticas costaron a las víctimas individuales al menos 1.300 millones de dólares. En 2022, el gobierno de Costa Rica se vio obligado a declarar el estado de emergencia tras un ciberataque de ransomware que debilitó la infraestructura digital del país durante meses.

Los autores de delitos cibernéticos también son bastante heterogéneos. Van desde estafadores a pequeña escala hasta bandas transnacionales de cibercriminales e incluso actores patrocinados por los Estados. Los cibercriminales suelen atacar víctimas de distintas jurisdicciones nacionales, lo que convierte al cibercrimen en una amenaza global con impacto local. En los últimos tiempos se han vuelto cada vez más comunes los grupos de delincuencia organizada que ofrecen el cibercrimen como un servicio.

En este contexto, el objetivo que se persigue con el tratado es hacer frente al cibercrimen y mejorar la cooperación y coordinación entre los Estados.

4. ¿EN QUÉ CONSISTE EL PROCESO DEL TRATADO?

En diciembre de 2019, la ONU aprobó una resolución mediante la cual se estableció un Comité ad hoc (AHC: Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes) de participación abierta encargado de desarrollar una "convención internacional integral para contrarrestar el uso de las TIC con fines delictivos".

Las negociaciones comenzaron a principios de 2022. La agenda del tratado consta de seis sesiones de negociación, tres en Viena y tres en Nueva York. En cada reunión se han abordado distintas partes del tratado, entre ellas los capítulos sobre la criminalización, las medidas procesales, el papel de los cuerpos de seguridad de los Estados, la cooperación internacional, la asistencia técnica, las medidas preventivas y la implementación.

Se espera que los Estados lleguen a un consenso en las negociaciones, pero si esto no es posible, se aplicarán las normas de votación por mayoría de dos tercios. En las dos sesiones más recientes se crearon grupos de trabajo informales para que los Estados debatieran sobre asuntos controvertidos. En junio, la presidencia del Comité publicó el borrador del texto de la convención, el cual será sometido a discusión por parte de los Estados en agosto de 2023.

Aunque los Estados son los responsables de negociar, adoptar, ratificar y aplicar el tratado, la sociedad civil y el sector privado han desempeñado un papel fundamental en la gestación del convenio mediante declaraciones, consultas y eventos complementarios.

5. ¿CUÁLES SON LOS ÁMBITOS EN LOS QUE SE PRESENTAN MAYORES DESACUERDOS?

El proceso para negociar el tratado es complejo. El borrador del texto es la síntesis de meses de negociaciones y cientos de enmiendas propuestas, y consta de nueve capítulos y más de sesenta artículos.

Los ámbitos en los que se presentan mayores desacuerdos que se abordan en este documento están relacionados con el alcance del tratado, las garantías en materia de derechos humanos, el modo de abordar las brechas en las capacidades de los Estados, la forma en que el tratado debe armonizarse con otros instrumentos y la importancia del género en el mismo.

Este artículo no se ocupa de cuestiones como la protección de datos o el papel del sector privado y la sociedad civil. Asimismo, destaca únicamente algunos de los muchos desacuerdos terminológicos.

Además, el proceso del AHC coincidió con el inicio de la invasión a gran escala de Ucrania por parte de Rusia. Muchos representantes estatales han condenado la agresión rusa y se preguntan si pueden negociar con Rusia de buena fe.

6. ¿QUÉ CIBERCRÍMENES DEBE ABORDAR EL TRATADO?

Algunos Estados abogan por un tratado que criminalice los delitos que dependen del entorno cibernético y una amplia gama de delitos que son facilitados por ese entorno, entre ellos los delitos basados en el contenido. En el lado más extremo del espectro se encuentra un grupo de países que incluye a Rusia, Bielorrusia, China, Nicaragua y Cuba, cuyas propuestas han incluido sugerencias muy polémicas para que se criminalice la "incitación a actividades subversivas o armadas" y la "coacción al suicidio" por medio de las TIC. China ha propuesto criminalizar la "difusión de información falsa [...] que pueda dar lugar a graves desórdenes sociales", mientras que India ha abogado por criminalizar las infracciones relacionadas con el "ciberterrorismo".

Otros Estados –incluidos los Estados miembros de la Unión Europea, Estados Unidos, el Reino Unido, Japón y Australia– quieren incluir los principales delitos que dependen del entorno cibernético y un número muy limitado de aquellos delitos tradicionales que son facilitados por el entorno cibernético y que se han transformado drásticamente gracias a las tecnologías digitales, siendo el principal ejemplo de estos últimos los delitos relacionados con el abuso y la explotación sexual de menores (Material de abuso sexual de menores; CSAM: Child Sexual Abuse Materials). Estos Estados argumentan que un tratado con una larga lista de infracciones facilitadas por el entorno cibernético puede ser objeto de malos usos o de interpretaciones erróneas.

Los enfoques sobre la criminalización afectan también el alcance general del tratado. Los Estados partidarios de un enfoque restringido han expresado su disposición a considerar acuerdos más integrales sobre cooperación internacional y otros capítulos: por ejemplo, que el tratado sirva de base para el intercambio de material probatorio entre jurisdicciones en relación con cualquier delito que incluya un componente de pruebas digitales, y no solo con los delitos contemplados en el instrumento.

Algunos Estados también discrepan con respecto a la terminología que se utiliza para describir el tratado en sí, argumentando que la frase que figura en el título del AHC –"el uso de las TIC con fines delictivos"– apoya un enfoque expansivo de la criminalización, ya que podría referirse a cualquier actividad delictiva en la que se haya utilizado un dispositivo TIC. Hoy en día, esto podría incluir casi todos los delitos. Aunque el término " cibercrimen" sigue siendo ambiguo, en general se considera más restringido.

> *"Aunque la mayoría de los Estados están de acuerdo con que los compromisos en materia de derechos humanos son esenciales, algunos alegan que el tratado no es un tratado de derechos humanos, por lo que las alusiones a estos deberían reducirse al mínimo".*

Un tratado con una larga lista de delitos –especialmente aquellos relacionados con los contenidos– aumenta la probabilidad de duplicaciones y contradicciones entre los marcos existentes y pone en peligro la libertad de expresión y otros derechos humanos al criminalizar los contenidos en Internet. Existe también el riesgo de que actividades legítimas como las de los investigadores de seguridad informática, los "hackers de sombrero blanco" y los investigadores de campo se criminalicen inadvertidamente.

Aunque las negociaciones siguen en curso, el borrador del texto publicado en junio adopta un enfoque relativamente restringido de la criminalización.

7. ¿CÓMO Y POR QUÉ DEBE PROTEGER EL TRATADO LOS DERECHOS HUMANOS?

Las medidas destinadas a combatir al cibercrimen pueden poner en peligro los derechos humanos. Algunos Estados han utilizado las leyes contra el cibercrimen para criminalizar los contenidos en Internet y limitar la libertad de expresión arremetiendo contra periodistas, activistas y opositores políticos o para vigilar el compor-

tamiento mediante las llamadas "cláusulas de moralidad".

Además, las investigaciones sobre cibercrimen pueden resultar muy invasivas. La interceptación y recopilación de datos de tráfico de las comunicaciones electrónicas por parte de los organismos encargados de velar por el cumplimiento de la ley puede plantear riesgos para la privacidad, al igual que el tratamiento indebido de datos personales sensibles.

Aunque la mayoría de los Estados está de acuerdo con que los compromisos en materia de derechos humanos son esenciales, algunos alegan que el tratado no es uno de derechos humanos, por lo que las alusiones a estos deberían reducirse al mínimo. Para algunos Estados, esto significa incluir un solo artículo sobre derechos humanos en el capítulo que abre el tratado, sin hacer referencia a derechos o marcos específicos. Para otros, esto significa incluir referencias explícitas a tratados específicos y reiterar los compromisos en materia de derechos humanos a lo largo del convenio cuando sea necesario.

Hay un grupo minoritario de Estados que se opone a cualquier referencia a los derechos humanos. Suelen citar las convenciones de la ONU contra la corrupción y la delincuencia organizada transnacional, que han demostrado su eficacia sin asumir compromisos en materia de derechos humanos.

Las partes interesadas en la sociedad civil, entre ellas Chatham House, han destacado la importancia de que se incluyan varias referencias específicas a los derechos humanos y a la protección de la infancia, ya que estas establecen expectativas claras y compromisos vinculantes para los Estados que apliquen el tratado.

El borrador del texto de la convención insta a los Estados a que velen por la coherencia entre la aplicación del tratado y el cumplimiento de sus obligaciones en virtud del derecho internacional de los derechos humanos. Sin embargo, no hace referencia a instrumentos específicos, aparte de una sola mención a la Convención sobre los derechos de los niños y niñas en el subartículo sobre la protección de los niños y niñas acusados de delitos relacionados con material de abuso sexual de menores [CSAM].

8. ¿CÓMO DEBERÍA ABORDAR EL TRATADO LAS BRECHAS EN MATERIA DE CAPACIDAD?

Existen asimetrías globales en las capacidades de los Estados (incluyendo la financiación y los recursos) y en las aptitudes necesarias para luchar contra el cibercrimen. Los países en desarrollo son desproporcionadamente vulnerables a los impactos directos e indirectos del cibercrimen, por lo que el desarrollo de capacidades es una prioridad urgente.

El capítulo del tratado sobre asistencia técnica describe las obligaciones y expectativas que se tienen de los Estados miembro a la hora de abordar las brechas en materia de capacidad. Algunos países en desarrollo han solicitado compromisos de transferencia de tecnología, que podrían incluir tecnologías de "doble uso" con aplicaciones tanto civiles-comerciales como armamentísticas-militares. Otros han rechazado estas propuestas, aludiendo a la preocupación que suscita el margen de posibles abusos.

> *"Los países en desarrollo son desproporcionadamente vulnerables a los impactos directos e indirectos del cibercrimen, por lo que el desarrollo de capacidades es una prioridad urgente".*

Independientemente de la terminología, aunque el desarrollo de capacidades y la asistencia técnica son importantes, también tienen sus propios riesgos, como los riesgos para los derechos humanos derivados del uso indebido y deliberado de herramientas de doble uso; los daños no deliberados derivados de una capacitación inadecuada o deficiente, y el refuerzo de las desigualdades globales existentes por medio de acuerdos condicionados. Es esencial arraigar el desarrollo de capacidades en principios consolidados y compartidos, como los propuestos por el Grupo de Trabajo de Participación Abierta de las Naciones Unidas sobre ciberseguridad.

Varios países desarrollados han insistido también en que la asistencia técnica debe prestarse de forma voluntaria y no prescriptiva.

9. ¿CÓMO DEBERÍA ARMONIZARSE EL TRATADO CON OTRAS INICIATIVAS YA EXISTENTES?

Aunque un nuevo tratado podría convertirse en una herramienta valiosa dentro del esfuerzo global contra el cibercrimen, debe armonizarse con los mecanismos y las redes internacionales existentes que ocupan espacios similares.

Las convenciones de la ONU contra la delincuencia transnacional organizada y la corrupción, ratificadas por casi todos los Estados miembro, constituyen una parte importante de las respuestas mundiales a la delincuencia transnacional. Muchos Estados sugieren tomar prestados –y adaptar– artículos de estos instrumentos para el tratado sobre cibercrimen.

Los desacuerdos más profundos se refieren a los instrumentos existentes contra el cibercrimen. Desde hace más de veinte años, y con casi setenta Estados miembro, el Convenio de Budapest del Consejo de Europa ha intentado definir qué se considera cibercrimen y cómo deben cooperar los organismos encargados de velar por el cumplimiento de la ley. Muchos Estados han desarrollado su legislación a partir de este Convenio.

Pero no todos los países lo han ratificado. Algunos –como Rusia– han dicho reiteradamente que la Convención de Budapest no es relevante a escala mundial y que amenaza principios como la soberanía de los Estados y la no intervención. Esto los llevó a impulsar la resolución que estableció el Comité ad hoc [AHC], la cual fue aprobada a pesar de la oposición de muchos Estados occidentales y representantes de la sociedad civil.

Las propuestas de los Estados en el proceso de negociación del tratado también han hecho referencia a disposiciones de instrumentos regionales, como la Convención de la Unión Africana sobre ciberseguridad y protección de datos personales.

10. ¿CÓMO HA ESTADO PRESENTE EL GÉNERO EN LAS NEGOCIACIONES DE LOS TRATADOS?

Estados como Canadá, Chile y el Reino Unido han apoyado una alusión a la "incorporación de una perspectiva de género" como parte del artículo sobre derechos humanos del tratado, aduciendo que este lenguaje reforzaría y haría más incluyente el instrumento contra el cibercrimen. Este sería el caso debido a que las personas con diferentes identidades de género se exponen a riesgos específicos cuando se enfrentan al cibercrimen y a la gobernanza del cibercrimen, particularmente en jurisdicciones en las que las identidades y expresiones LGBTQI+ en sí se criminalizan.

Así pues, estos Estados también abogan por incorporar la perspectiva de género en todo el tratado. Por ejemplo, si se reforzara un artículo sobre extradición incorporando un lenguaje sobre identidad de género, el Estado miembro requerido podría denegar una solicitud de extradición en caso de que considere que un delincuente podría ser condenado a causa de su género.

Otros Estados siguen oponiéndose rotundamente a cualquier mención de género en el tratado. Algunos han argumentado que los Estados definen el sexo y el género de forma diferente, por lo que es imposible llegar a un consenso sobre las referencias a la igualdad de género, mientras que otros han cuestionado la priorización de la protección de las mujeres y las niñas por encima de otros grupos vulnerables.

Los distintos géneros experimentan de diversas formas los delitos que dependen del entorno cibernético y los que son facilitados por el entorno cibernético, así como las "prácticas, instituciones y políticas asociadas". Un futuro instrumento eficaz contra el cibercrimen debe tener en cuenta los daños, riesgos y experiencias de todos los géneros.

11. ¿QUÉ VIENE DESPUÉS?

Tras haberse celebrado cinco de las seis sesiones de negociación, las negociaciones han llegado a una fase crucial. En agosto de 2023 los representantes de los Estados

se reunirán en Nueva York para debatir el borrador del texto de la convención, que es la base del tratado final. Las negociaciones continuarán a principios de 2024 con el objetivo de adoptar el tratado durante la Asamblea General de la ONU en septiembre de ese año.

El equipo encargado de política cibernética de Chatham House continuará siguiendo de cerca las negociaciones y ofrecerá un análisis sobre los principales hitos y cuestiones abordadas.

CONTACTO

Friedrich-Ebert-Stiftung (FES)

Calle 71 nº 11-90 | Bogotá-Colombia

Teléfono (+57 1) 601 347 30 77 / 601 347 30 92

catalina.nino@fes.de

https://colombia.fes.de