

Bruselas, 1 de abril de 2022
(OR. en)

7860/22
ADD 1

CYBER 108
COPEN 118
JAI 444
COPS 143
RELEX 429
JAIEX 30
TELECOM 138
POLMIL 82
CFSP/PESC 432
ENFOPOL 179
DATAPROTECT 95

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D. ^a Martine DEPREZ, directora
Fecha de recepción:	29 de marzo de 2022
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.º doc. Ción.:	COM(2022) 132 final
Asunto:	ANEXO de la Recomendación de Decisión del Consejo por la que se autorizan las negociaciones de un convenio internacional integral sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos

Adjunto se remite a las Delegaciones el documento – COM(2022) 132 final.

Adj.: COM(2022) 132 final

Bruselas, 29.3.2022
COM(2022) 132 final

ANNEX

ANEXO

de la

Recomendación de Decisión del Consejo

**por la que se autorizan las negociaciones de un convenio internacional integral sobre la
lucha contra la utilización de las tecnologías de la información y la comunicación con
fines delictivos**

ANEXO

Por lo que respecta al proceso de las negociaciones, la Unión debe aspirar a lo siguiente:

- 1) Que el proceso de negociación sea abierto, inclusivo y transparente y que se base en la cooperación de buena fe.
- 2) Que el proceso de negociación permita la participación significativa de todas las partes interesadas, incluida la sociedad civil, el sector privado, el mundo académico y las organizaciones no gubernamentales.
- 3) Que todas las aportaciones recibidas de todos los miembros de las Naciones Unidas se examinen en igualdad de condiciones para garantizar la inclusividad del proceso.
- 4) Que el proceso de negociación se base en un programa de trabajo eficaz y realista.

Por lo que respecta a los objetivos generales de las negociaciones, la Unión debe aspirar a lo siguiente:

- 5) El Convenio constituye un instrumento eficaz para las autoridades policiales y judiciales en la lucha mundial contra la ciberdelincuencia, con el objetivo de añadir valor a la cooperación internacional.
- 6) Se tiene plenamente en cuenta el marco existente de instrumentos y esfuerzos internacionales y regionales probados, tal como se refleja en las Resoluciones 74/247 y 75/282 de la Asamblea General de las Naciones Unidas. En consecuencia, el Convenio es compatible con los instrumentos internacionales existentes y los complementa, en particular el Convenio del Consejo de Europa sobre la Ciberdelincuencia celebrado en Budapest en 2001 y sus protocolos, la Convención de las Naciones Unidas de 2000 contra la Delincuencia Organizada Transnacional y sus protocolos, así como otros instrumentos internacionales y regionales pertinentes. El Convenio evita cualquier impacto en su aplicación o en la futura adhesión de cualquier país a ellos y, en la medida de lo posible, evita duplicaciones innecesarias.
- 7) Se tienen plenamente en cuenta el trabajo y los resultados del Grupo Intergubernamental de Expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético, tal como se acordó en la Resolución 75/282 de la Asamblea General de las Naciones Unidas.
- 8) Las disposiciones del Convenio garantizan la máxima protección posible de los derechos humanos. Los Estados miembros de la UE deben poder cumplir con el Derecho de la UE, incluidos sus derechos fundamentales, libertades y principios generales consagrados en los Tratados de la Unión Europea y en la Carta de los Derechos Fundamentales. Las disposiciones del Convenio también deben ser compatibles con las obligaciones comerciales internacionales de la UE y sus Estados miembros.

Por lo que respecta a la sustancia de las negociaciones, la Unión debe aspirar a lo siguiente:

- 9) Que el Convenio defina los delitos que solo pueden cometerse mediante sistemas de información.
- 10) Que el Convenio defina los delitos que pueden cometerse sin utilizar sistemas de información, pero que pueden fomentarse mediante sistemas de información en

determinadas circunstancias, pero solo en los casos en que la participación de los sistemas de información modifique sustancialmente las características o el impacto de las infracciones.

- 11) Que los delitos se definan de forma clara, estricta y tecnológicamente neutra. Que las definiciones sean compatibles con las de otros convenios internacionales o regionales pertinentes, en particular en el ámbito de la delincuencia organizada o la ciberdelincuencia, y con las normas internacionales en materia de derechos humanos.
- 12) Que el Convenio establezca normas sobre la tentativa y la complicidad de tales delitos, sobre la responsabilidad de las personas jurídicas por tales delitos, sobre el establecimiento de la jurisdicción sobre tales delitos y sobre las sanciones y medidas en relación con tales delitos que sean compatibles con otros convenios internacionales o regionales pertinentes, en particular en el ámbito de la delincuencia organizada o la ciberdelincuencia, y con las normas internacionales en materia de derechos humanos.
- 13) Que el Convenio fije medidas penales procesales que permitan a las autoridades investigar eficazmente los ciberdelitos, inmovilizar y decomisar el producto de tales delitos y conservar u obtener pruebas electrónicas de cualquier delito penal en el marco de una investigación o un procedimiento penal, teniendo debidamente en cuenta el principio de proporcionalidad.
- 14) Que estas medidas penales procesales aporten un valor añadido suficiente en comparación con otros convenios internacionales o regionales pertinentes, en particular en el ámbito de la delincuencia organizada o la ciberdelincuencia, y sean compatibles con dichos convenios y con las normas internacionales en materia de derechos humanos.
- 15) Que las medidas procesales para conservar u obtener pruebas electrónicas contengan una definición clara y estricta del tipo de información abarcada. Que las medidas procesales para la cooperación con entidades del sector privado garanticen que la carga impuesta sobre dichas entidades sea proporcionada y que estas respeten plenamente los derechos humanos de sus usuarios. Que el Convenio proporcione claridad jurídica a los proveedores de servicios en línea (por ejemplo, los proveedores de servicios de internet) en sus interacciones con las autoridades policiales de los Estados miembros que sean Parte del Convenio. Que las medidas procesales para la retirada de contenidos ilícitos solo se refieran a aquellos que puedan ser lo bastante específicos y definirse de forma estricta.
- 16) Que el Convenio fije medidas de cooperación que permitan a las autoridades de los distintos Estados que sean parte del instrumento cooperar eficazmente a efectos de investigaciones o procedimientos penales relativos a delitos definidos en el instrumento, o cooperar para conservar u obtener pruebas electrónicas de cualquier delito en el marco de una investigación o un procedimiento penal.
- 17) Que estas medidas de cooperación aporten un valor añadido suficiente en comparación con otros convenios internacionales o regionales pertinentes, en particular en el ámbito de la delincuencia organizada o la ciberdelincuencia, y sean compatibles con dichos convenios y con las normas internacionales en materia de derechos humanos.
- 18) Que las medidas de cooperación estén sujetas a las condiciones dispuestas en la legislación de la parte requerida y prevean motivos amplios de denegación, tales como garantizar la protección de los derechos fundamentales, incluido el derecho a la

protección de los datos personales, también en el contexto de las transferencias de datos personales, y, en su caso, la existencia de una doble tipificación.

- 19) Que el Convenio fije condiciones estrictas y garantías sólidas para garantizar que los Estados miembros de la UE puedan respetar y proteger los derechos fundamentales, las libertades y los principios generales del Derecho de la UE consagrados en los Tratados de la Unión Europea y en la Carta de los Derechos Fundamentales, incluidos, en particular, el principio de proporcionalidad, las garantías y derechos procesales, el derecho a la tutela judicial efectiva, la presunción de inocencia, el derecho a un juicio justo y los derechos de defensa de las personas sujetas a procedimientos penales, así como el derecho a la intimidad, el derecho a la protección de los datos personales y de las comunicaciones electrónicas cuando se traten dichos datos, incluidas las transferencias a autoridades de países no pertenecientes a la Unión Europea, y el derecho a la libertad de expresión e información. Que el Convenio garantice, en particular, que los Estados miembros de la UE puedan cumplir con los requisitos para las transferencias internacionales de datos personales en el sentido de la Directiva (UE) 2016/680, el Reglamento (UE) 2016/679 y la Directiva 2002/58/CE. Que las condiciones y garantías también garanticen la protección de los derechos humanos y las libertades fundamentales en consonancia con las normas internacionales en materia de derechos humanos. Que esto se aplique a todo el Convenio, incluidas las medidas procesales y de cooperación, también las que pueden interferir significativamente en los derechos de las personas, como el embargo preventivo y el decomiso de los productos del delito y la extradición.
- 20) Que el Convenio sirva de base para medidas voluntarias de desarrollo de capacidades a fin de apoyar a los países en su capacidad para llevar a cabo investigaciones y procedimientos eficaces en materia de ciberdelincuencia, y obtener pruebas electrónicas para las investigaciones y procedimientos de otros delitos, incluso mediante asistencia técnica y formación. Que la UNODC tenga un papel claramente descrito en la aplicación de dichas medidas.
- 21) Que el Convenio tenga debidamente en cuenta la posición de las personas físicas y jurídicas como víctimas de la ciberdelincuencia. Que el Convenio garantice que estas reciben la asistencia, el apoyo y la protección adecuados.
- 22) Que el Convenio sirva de base para medidas prácticas de prevención de la ciberdelincuencia claramente definidas, estrictamente limitadas y distintas de las medidas procesales penales que podrían interferir en los derechos y libertades de las personas físicas o jurídicas.

Por lo que respecta al funcionamiento del Convenio, la Unión debe aspirar a lo siguiente:

- 23) Que el Convenio conserve los instrumentos mundiales y regionales existentes y la cooperación internacional en curso en la lucha mundial contra la ciberdelincuencia. En particular, que los Estados miembros de la Unión Europea, en sus relaciones mutuas, puedan seguir aplicando las normas de la Unión Europea.
- 24) Que el Convenio establezca un mecanismo adecuado para garantizar su aplicación e indicar las disposiciones finales, incluidas las relativas a la solución de diferencias, la firma, la ratificación, la aceptación, la aprobación y la adhesión, la entrada en vigor, la modificación, la suspensión, la denuncia y el depósito, así como las lenguas, que se inspiren, cuando sea posible y apropiado, en las disposiciones de otros convenios

internacionales o regionales pertinentes, en particular en el ámbito de la delincuencia organizada o la ciberdelincuencia.

- 25) Que el Convenio permita a la Unión Europea formar parte de él.