Versión 18 septiembre 2023

Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios

Convenio sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia ("Convenio de Budapest") se considera la norma internacional más completa hasta la fecha, ya que proporciona un marco integral y coherente en contra del ciberdelito y la evidencia electrónica. Sirve como una guía para cualquier país que desea desarrollar una legislación nacional integral sobre ciberdelitos y como un marco para la cooperación internacional entre los Estados Parte de este tratado.

El Convenio de Budapest prevé: (i) la criminalización de la conducta, que va desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil; (ii) herramientas de derecho procesal para hacer más efectiva la investigación relacionada con ciberdelitos y la obtención de evidencias electrónicas; y (iii) una cooperación internacional mas ágil y eficiente. El tratado está abierto para la adhesión de cualquier país.

El Convenio se completa con un Primer Protocolo Adicional relativo a la penalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (STCE 189) y un Segundo Protocolo Adicional relativo a la cooperación internacional reforzada y la divulgación de pruebas electrónicas (STCE 224).

Los Estados que participaron en la negociación del Convenio (miembros del Consejo de Europa, y Canadá, Japón, Sudáfrica y EE.UU.) pueden firmar y ratificar el tratado. En virtud del artículo 37, cualquier otro Estado puede convertirse en Parte mediante "adhesión" si está dispuesto a aplicar las disposiciones de este tratado.

El procedimiento de adhesión implica:

1. Una vez que esté disponible un proyecto de ley que indique que un Estado ya ha implementado o es posible que pueda implementar las disposiciones del Convenio de Budapest en su legislación nacional, el Ministro de Relaciones Exteriores (u otro representante autorizado) deberá enviar una carta dirigida al Secretario General del Consejo de Europa en la que manifieste el interés de su Estado en adherirse al Convenio de Budapest.Una vez que exista consenso entre los actualesEstados Partes del Convenio, se invitará al Estado a adherirse.

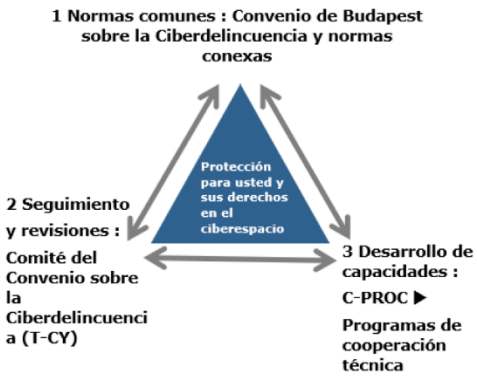
Las autoridades de ese Estado deberán formalizar sus procedimientos internos similares a la ratificación de cualquier tratado internacional antes de depositar el instrumento de adhesión ante el Consejo de Europa.El resultado final es el mismo, ya sea la ratificación o la adhesión. Las Partes en el

Convenio también pueden ser Partes en los dos Protocolos sin necesidad de una nueva solicitud de adhesión.

En septiembre de 2023, 68 Estados eran Partes en el Convenio (países europeos, así como Argentina, Australia, Brasil, Cabo Verde, Canadá, Chile, Colombia, Costa Rica, Estados Unidos, Filipinas, Ghana, Israel, Japón, Marruecos, Mauricio, Nigeria, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga), otros 2 países lo han firmado (Irlanda y Sudáfrica) y 19 han sido invitados a adherirse (Benín, Burkina Faso, Camerún, Costa de Marfil, Ecuador, Corea, Fiyi, Guatemala, Kazakstán, Kiribati, México, Nueva Zelanda, Níger, Sierra Leona, Timor Oriental, Trinidad y Tobago, Túnez, Uruguay y Vanuatu).

Estos 89 Estados participan como miembros (Partes) u observadores (signatarios o invitados) en el Comité del Convenio sobre la Ciberdelincuencia (T-CY).

El T-CY, entre otras cosas, evalúa la aplicación del Convenio por las Partes, adopta Notas Orientativas o prepara instrumentos jurídicos adicionales.



Los programas de Creación de Capacidad, administrados por la Oficina especializada del Programa sobre Ciberdelincuencia del Consejo de Europa (C-PROC) en Rumania, ayuda a países en distintas partes del mundo a desarrollar las capacidades necesarias para implementar el Convenio de Budapest o para adoptar las recomendaciones del Comité del Convenio sobre la Ciberdelincuencia (T-CY).

Beneficios para los Estados Parte

Cualquier país puede hacer uso del Convenio sobre la Ciberdelincuencia como directriz, lista de control o ley modelo, y un gran número ya hace uso de esta oportunidad. Sin embargo, convertirse en Parte de este tratado conlleva ventajas adicionales:

- El Convenio establece un **marco legal para la cooperación internacional** no sólo en relación con la ciberdelincuencia (delitos contra y por medio de ordenadores), sino con cualquier delito que implique pruebas electrónicas.
- Las Partes del Convenio pueden firmar y ratificar el Segundo Protocolo Adicional al Convenio de Budapest, que proporciona **herramientas adicionales y aceleradas para mejorar la cooperación y la divulgación de pruebas electrónicas**, como la cooperación directa con los proveedores de servicios a través de las fronteras o la cooperación en situaciones de emergencia.
- Los Estados Partes podrán ser **miembros del Comité del Convenio sobre la Ciberdelincuencia (T-CY)** e intercambiar información y experiencias, evaluar la aplicación del Convenio o lo interpretar mediante Notas de orientación.

- Aunque un Estado no haya participado en la negociación del tratado original, como nueva Parte puede participar en la **negociación de futuros instrumentos** y en la evolución posterior del Convenio.
- Los Estados Partes del Convenio se comprometen entre sí para **una cooperación confiable y eficiente.** Las evidencias indican que es más probable que las entidades del sector privado cooperen con las autoridades de justicia penal de los Estados Partes del Convenio, dado que los Estados Partes deben contar con un marco jurídico nacional vigente sobre ciberdelitos y evidencias electrónicas, incluidas las salvaguardas previstas en el Artículo 15.
- Los Estados Partes que soliciten la adhesión o que se hayan adherido pueden convertirse en **países prioritarios para los programas de desarrollo de capacidades**. Dicha asistencia técnica es para facilitar la plena aplicación del Convenio y mejorar la capacidad de cooperación internacional.

Después de 20 años desde que se abrió el Convenio para su firma, la experiencia demuestra que no existen desventajas en formar parte de este tratado.

Primer Protocolo Adicional sobre xenofobia y racismo

El Primer Protocolo Adicional relativo a la penalización de actos de carácter racista y xenófobo cometidos por medio de sistemas informáticos (STCE 189) supone una ampliación del ámbito de aplicación del Convenio sobre la Ciberdelincuencia, incluidas sus disposiciones sustantivas, procesales y de cooperación internacional, para abarcar también los delitos de propaganda racista o xenófoba. Así pues, aparte de armonizar los elementos de derecho sustantivo de tales conductas, el Protocolo pretende mejorar la capacidad de las Partes para hacer uso de los medios y vías de cooperación internacional establecidos en el Convenio en este ámbito.

Las ventajas para las Partes son:

- **Un marco jurídico más sólido:** el Protocolo refuerza el marco jurídico de la lucha contra la xenofobia y el racismo en el ciberespacio proporcionando un conjunto claro de directrices para la tipificación de estos delitos.
- **Mayor cooperación internacional:** el Protocolo promueve la cooperación internacional en la investigación y persecución de delitos relacionados con la xenofobia y el racismo en línea, lo que es especialmente importante dado el carácter transfronterizo de muchos de estos delitos.
- **Mayor protección para las víctimas:** la penalización de la xenofobia y el racismo en línea permite a las víctimas buscar justicia y recibir apoyo.

El Primer Protocolo Adicional se abrió a la firma el 28 de enero de 2003. En septiembre de 2023, 35 Estados eran Partes y otros 10 habían firmado el Primer Protocolo.

Segundo Protocolo adicional sobre pruebas electrónicas

Considerando la proliferación de la ciberdelincuencia y la creciente complejidad de la obtención de pruebas electrónicas que pueden estar almacenadas en jurisdicciones extranjeras, múltiples,

cambiantes o desconocidas, las competencias de las autoridades de la justicia penal se ven limitadas por las fronteras territoriales. Como resultado, sólo una parte muy pequeña de la ciberdelincuencia que se denuncia a las autoridades policiales desemboca en decisiones judiciales. Como respuesta, el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia (STCE 224) establece una base jurídica para la divulgación de la información de registro de nombres de dominio y para la cooperación directa con los proveedores de servicios de información sobre abonados, medios eficaces para obtener información sobre abonados y datos de tráfico, cooperación inmediata en casos de emergencia, herramientas de asistencia mutua, así como salvaguardias de protección de datos personales.

Entre las principales características del Protocolo figuran:

- Solicitud directa a registradores de otras jurisdicciones para obtener información sobre el registro de nombres de dominio
- Órdenes directas a proveedores de servicios de otras jurisdicciones para obtener información sobre los abonados
- Medios más eficaces para obtener información sobre abonados y datos de tráfico mediante la cooperación entre gobiernos
- Cooperación expeditiva en situaciones de emergencia
- Equipos conjuntos de investigación e investigaciones conjuntas
- Videoconferencias.

El Segundo Protocolo Adicional se abrió a la firma el 12 de mayo de 2022. En septiembre de 2023, 42 Estados habían firmado el Segundo Protocolo (Albania, Alemania, Andorra, Argentina, Austria, Bélgica, Bulgaria, Cabo Verde, Canadá, Chile, Colombia, Costa Rica, Croacia, Eslovenia, España, Estados Unidos de América, Estonia, Finlandia, Francia, Ghana, Grecia, Hungría, Islandia, Italia, Japón, Lituania, Luxemburgo, Malta, Marruecos, Mauricio, Montenegro, Macedonia del Norte, Países Bajos, Portugal, Reino Unido, República de Moldova, República Dominicana, Rumanía, Serbia, Sri Lanka, Suecia y Ucrania) y 2 Estados lo habían ratificado (Japan y Serbia).

Contacto

Consejo de Europa
División de Ciberdelincuencia, DGI

Estrasburgo, Francia
Correo electrónico:
cybercrime@coe.int

www.coe.int/cybercrime