

**APROBACIÓN DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO
SOBRE LA CIBERDELINCUENCIA, RELATIVO A LA COOPERACIÓN
REFORZADA Y LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS**

EXPEDIENTE N° 24.783

DICTAMEN NEGATIVO DE MINORÍA

11 DE JULIO DE 2025

**CUARTA LEGISLATURA
SEGUNDO PERIODO DE SESIONES EXTRAORDINARIAS**

ÁREA DE COMISIONES LEGISLATIVAS I

DEPARTAMENTO DE COMISIONES LEGISLATIVAS

**APROBACIÓN DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO
SOBRE LA CIBERDELINCUENCIA, RELATIVO A LA COOPERACIÓN
REFORZADA Y LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS**

DICTAMEN NEGATIVO DE MINORÍA

EXPEDIENTE N° 24.783

Asamblea Legislativa:

El suscrito Diputado ANTONIO JOSÉ ORTEGA GUTIÉRREZ integrante de la Comisión Permanente Ordinaria de Relaciones Internacionales y Comercio Exterior, rindo el presente Dictamen Negativo de Minoría sobre el proyecto, APROBACIÓN DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA, RELATIVO A LA COOPERACIÓN REFORZADA Y LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS, Expediente legislativo N° 24.783, iniciativa de ley del poder ejecutivo, publicado en la Gaceta N° 24 del 06 de febrero de 2025, con base en las siguientes consideraciones.

2. RESUMEN

Por medio de este proyecto de Ley se propone la aprobación del Segundo Protocolo o Adicional al Convenio sobre la Ciberdelincuencia, Relativo a la Cooperación Reforzada y la divulgación de Pruebas Electrónicas, Adicional al Convenio de Budapest sobre Ciberdelincuencia.

Costa Rica suscribió y ratificó en el año 2001 el Convenio de Budapest que es el principal Convenio sobre Ciberdelincuencia, negociado en el seno del Consejo de Europa. Este Segundo Protocolo adicional al Convenio, relativo al refuerzo de la cooperación y divulgación de pruebas electrónicas, este Protocolo fue adoptado por el Comité de Ministros del Consejo de Europa en la reunión 1417bis del 17 de noviembre de 2021 de los Delegados de los Ministros, abriéndose para su firma en Estrasburgo a partir del 12 de mayo del 2022 y que entrará en vigencia una vez que 5 estados lo ratifiquen.

Este segundo protocolo busca una modernización de la cooperación internacional en ciberdelincuencia y evidencias electrónicas, facilitando el acceso transfronterizo a pruebas digitales como lo es el acceso a datos en la nube, además permite la cooperación directa con proveedores, permitiendo que empresas tecnológicas en otros países puedan solicitar datos electrónicos sin pasar por vías diplomáticas, así también frente a solicitudes que se declaren urgentes permite el acceso de procesos acelerados.

En este protocolo requiere cinco ratificaciones para entrar en vigor a nivel internacional, lo que actualmente no ha sucedido.

El expediente N° 24.783 se resume a continuación:

I. ASPECTOS DE TRÁMITE PARLAMENTARIO:

- a) El día 20 de enero del 2025, el Poder Ejecutivo, con firma de la Ministra Laura Fernández Delgado desde el Ministerio de la Presidencia, presentaron ante la Secretaría del Directorio, el proyecto de ley denominado **“APROBACIÓN DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA, RELATIVO A LA COOPERACIÓN REFORZADA Y LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS”**
- b) El día 28 de enero del 2025, el Departamento de Archivo, Investigación y Trámite procedió a remitir a la Imprenta Nacional, la iniciativa de ley para su respectiva publicación, de conformidad con lo que establece el artículo 117 del Reglamento de la Asamblea Legislativa.
- c) El día 13 de febrero del 2025 la Comisión Permanente Especial de Relaciones Internacionales recibe la iniciativa de ley del Departamento de Archivo, Investigación y Trámite, para su estudio y posterior dictamen.
- d) El día 19 de febrero del 2025, el expediente legislativo en cuestión ingresó al orden del día y debate de la Comisión Permanente Especial de Relaciones Internacionales.
- e) El día 26 de febrero del año 2025, en sesión ordinaria de la Comisión, la iniciativa de ley se consulta a distintas instituciones públicas y organizaciones, al igual que el 05 de marzo del año en mención.

II. CONSULTAS REALIZADAS:

Tomando en consideración la pertinencia con esta propuesta de ley, la misma fue consultada a las siguientes entidades:

- Poder Judicial
- Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)
- Ministerio de Relaciones Exteriores y Culto
- SUTEL
- Ministerio de Relaciones Exteriores y Culto.
- Ministerio de Ciencia y Tecnología.
- Ministerio de Seguridad Pública.

- Escuela de Relaciones Internacionales de la Universidad Nacional.
- Escuela de Ciencias Políticas de la Universidad de Costa Rica.
- Colegio de Profesionales en Ciencias Políticas y Relaciones Internacionales.
- Observatorio de la Política Nacional de la Universidad de Costa Rica.
- Instituto de Investigaciones Sociales de la Universidad de Costa Rica.

III. **RESPUESTAS RECIBIDAS:**

| Institución/ Organización | Respuesta |
|---|--|
| Ministerio de Relaciones Exteriores y Culto | “Desde el MREC se valora con mucho interés la aprobación de este Segundo Protocolo al Convenio sobre la Ciberdelincuencia, ya que contribuirá a seguir robusteciendo las herramientas contra el cibercrimen que ha venido desarrollando en el país y, lo que es más importante, ampliará sus oportunidades y posibilidades para combatir el cibercrimen con sus contrapartes a nivel internacional.” |
| Corte Suprema de Justicia | “Se devuelve la consulta sin pronunciamiento de la Corte porque el texto consultado no se refiere a la organización o funcionamiento del Poder Judicial, supuestos que según regula el artículo 167 de la Constitución Política son los que requieren un pronunciamiento de la Corte Suprema de Justicia” |
| Autoridad Reguladora de los Servicios Públicos | “Una vez realizada la revisión respectiva, se determinó que la aprobación o no del proyecto de ley es un asunto de discrecionalidad legislativa, en el tanto no se afectan las atribuciones, competencias y potestades esenciales de la Autoridad Reguladora de los Servicios Públicos.” |
| Ministerio de Ciencia, Innovación, Tecnología y | “Posterior a una revisión del proyecto de ley, desde el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, debemos indicar que es de vital |

| | |
|-------------------------------------|---|
| Telecomunicaciones | <p>importancia avanzar pronto con este proceso de ratificación, por la relevancia del tema para la persecución de delitos informáticos y manejo de pruebas electrónicas.</p> <p>Este segundo protocolo operativiza y brinda instrumentos de procedimientos sobre lo relativo al tráfico, preservación, registro, confiscación entre otros a los proveedores de servicios y de dominio.”</p> |
| Organismo de Investigación Judicial | <p>“Con equivalencia de lo que se señala en la exposición de motivos del proyecto estudiado, actualmente la evidencia digital resulta un aspecto esencial y muy presente en las investigaciones penales, destacando entonces, la relevancia de contar con mecanismos eficaces para su aseguramiento y obtención, especialmente cuando dicha evidencia se encuentra fuera del territorio nacional. Con el paso del tiempo se ha venido detectando una mayor sofisticación de las estructuras criminales cuyo principal flagelo en el país ha estado representado por el vertiginoso crecimiento de los índices delictivos; siendo que dichas organizaciones operan a nivel internacional.”</p> |
| Ministerio de Seguridad Pública | <p>“no contiene aspectos que afecten la institucionalidad y funcionalidad del Ministerio de Seguridad Pública ni de sus cuerpos policiales adscritos, razón por la no se hace mayor análisis con respecto al proyecto por lo que no tenemos objeciones que oponer al mismo”</p> |
| Escuela de Ciencias Políticas | <p>Es importante recordar, que la Asamblea Legislativa aprobó el Convenio original sobre la ciberdelincuencia el 18 de mayo de 2017 y que el Poder Ejecutivo le dio el ejecútese y lo mandó a publicar el 26 de mayo del mismo año. De igual forma, el país firmó el Primer Protocolo adicional (2003) relativo a actos racistas y xenófobos, el cual entró en vigencia el 1 de marzo de 2006.</p> <p>En relación con el Segundo protocolo éste tiene por objeto luchar contra la ciberdelincuencia a nivel global, propiciar la cooperación internacional y facilitar la obtención de pruebas electrónicas en investigaciones o</p> |

| | |
|--|---|
| | <p>procesos penales relacionados con los ciberdelitos, salvaguardando los derechos fundamentales de las personas. El Segundo protocolo busca que los Estados puedan atender de forma más efectiva y coordinada las amenazas cibernéticas actuales y para ello permite a las autoridades competentes solicitar directamente a proveedores de servicios en otros países información sobre suscriptores y datos de tráfico, facilita la obtención de información de registro de nombres de dominio para identificar o contactar al titular, exige que las Partes (los Estados) mantengan registros adecuados del tratamiento de datos y aseguren mecanismos de supervisión independientes, introduce mecanismos más ágiles para la cooperación internacional, especialmente en situaciones de emergencia donde hay un riesgo inminente para la vida o seguridad de personas, permite reservas y 2 declaraciones específicas por parte de los Estados, y establece mecanismos para la enmienda y resolución de controversias.</p> <p>En general el Protocolo busca establecer mecanismos para luchar contra los ciberdelitos, resguardando la protección de los derechos humanos y fundamentales de las personas.</p> <p>Por lo señalado anteriormente, manifiesto mi acuerdo con la propuesta “Segundo protocolo adicional al convenio sobre la ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas”, Expediente 24.783.”</p> |
|--|---|

IV. INFORMTE DEL DEPARTAMENTO DE SERVICIOS TÉCNICOS:

Esta diputación rinde este dictamen en tiempo y forma, con el fin de cumplir con lo establecido por el artículo 80 del reglamento de la Asamblea Legislativa, para recomendar que se dictamine negativamente la presente iniciativa y proceder al archivo de la iniciativa.

Dado lo anterior, se hace la observación de que, al momento de la presentación de este dictamen, consta en el Sistema de Información Legislativa

(SIL) el estudio del Departamento de Servicios Técnicos, dentro de lo cual, destaca lo siguiente:

“Sobre las consideraciones de fondo; como punto importante a considerar indican que, corresponde a la Asamblea Legislativa “aprobar o improbar” el instrumento internacional sometido sin que sea válido modificar el contenido del Protocolo, esto por lo tanto no es una actividad legislativa ordinaria.

Sobre el análisis del articulado, se encuentra la observación sobre el error en la fecha que se indica en el artículo único del proyecto, en la razón de cierre del mismo Protocolo declara ser hecho y abierto a la firma el 12 de mayo de 2022. En el Estado de firmas y ratificaciones indica haber sido suscrito por Costa Rica el 13 de junio de 2022. En todo caso, los instrumentos internacionales se identifican por la fecha que ellos indican, y no por el eventual momento en que una Parte pueda haberlo o no suscrito. La recomendación de Servicios Técnicos es eliminar la fecha indicada. Aunado a lo indicado, el informe del Departamento de Servicios Técnicos indica que, la propuesta no tiene problema jurídico alguno e indican que su aprobación es un asunto de discrecionalidad política.

V. ANÁLISIS DE FONDO:

Se han encontrado aspectos a considerar sobre la aprobación de este protocolo, el cual, presenta objeciones de fondo, así como implicaciones en materia de derechos fundamentales como lo es a la información privada y personal y libertad de expresión. Si bien Costa Rica firmó en el año 2001 y ratifica en el 2012 el **Convenio de Budapest**, no ratificó en su momento el Primer Protocolo adicional al Convenio de Budapest “*Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de naturaleza racista o xenófoba cometidos por medio de sistemas informáticos*”, esta no adhesión al primer convenio es también una muestra que el **Convenio de Budapest** provee el marco necesario y suficiente para la cooperación sobre la ciberdelincuencia, **siendo los protocolos adicionales complementos no obligatorios** (según el propio artículo 39 del Convenio), además la aprobación es de carácter discrecional de la propia Asamblea.

Sobre estos protocolos, aún hay una ausencia de la necesidad práctica demostrada, **ya que no existe evidencia de que los protocolos resuelven vacíos operativos en el combate de la ciberdelincuencia**, además, Costa Rica cuenta con legislación en materia de ciberdelincuencia (Ley 9048 contra delitos informáticos), así como la protección de datos personales (Ley 8968) ya que incorpora mecanismos de cooperación internacional, esto hace que **la ratificación de protocolos adicionales no sea indispensable**, pues el país puede establecer acuerdos bilaterales o regionales específicos sin necesidad de adherirse a instrumentos multilaterales que limiten su soberanía digital, ya que este protocolo otorga facultades amplias a otros Estados para solicitar datos almacenados en Costa Rica sin garantizar reciprocidad o estándares equivalentes de protección de derechos, ante esto es fundamental que Costa Rica priorice la ratificación de

instrumentos que protejan derechos humanos antes de ampliar facultades de cooperación penal.

Algunas de las preocupaciones sobre este protocolo es el acceso a datos e información personal que se permite a los Estados sin pasar primero por los protocolos correspondientes que existen actualmente, esto representa un riesgo para la privacidad y la protección de datos ya que **permite el acceso transfronterizo sin suficientes garantías** que puede atentar contra el Reglamento General de Protección de Datos que regula el tratamiento de datos personales, ya que al haber posibilidades de solicitudes directas a empresas tecnológicas se permite que gobiernos extranjeros pidan datos a proveedores (como lo es Google) **sin supervisión judicial local** se debilita el control sobre cómo se usan esos datos. Además, las solicitudes aceleradas podrían usarse para **eludir garantías procesales en casos no justificados**, ya que existe un desequilibrio entre países en donde países con menos recursos técnicos o marcos legales obsoletos quedarían en desventaja para aplicar el protocolo o proteger a sus ciudadanos.

En síntesis, la no aprobación del protocolo no afecta la capacidad del país para combatir la ciberdelincuencia, preservando la soberanía en la regulación de pruebas digitales, la garantía de lo dispuesto en el Artículo 24 de la Constitución Política, así también permitiría mantener lo que indica el ordenamiento jurídico nacional en lo que refiere a ciberdelincuencia.

RECOMENDACIONES:

De conformidad con el análisis expuesto, así como aspectos técnicos de oportunidad y conveniencia, ésta diputación deja constancia que se abocó al estudio del **EXPEDIENTE N° 24.783 “APROBACIÓN DEL SEGUNDO PROTOCOLO ADICIONAL AL CONVENIO SOBRE LA CIBERDELINCUENCIA, RELATIVO A LA COOPERACIÓN REFORZADA Y LA DIVULGACIÓN DE PRUEBAS ELECTRÓNICAS”**, y que se recomendó a la Comisión Permanente Ordinaria de Relaciones Internacionales y Comercio Exterior que se **dictamine negativamente dicho expediente.**

Antonio Ortega Gutiérrez
Diputado