ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA

PODER EJECUTIVO

EXPEDIENTE N.º 18.484

DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS

PROYECTO DE LEY

APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA

Expediente N.° 18.484

ASAMBLEA LEGISLATIVA:

El Comité de Ministros del Consejo de Europa, en el curso de la reunión sostenida a nivel de delegados el 31 de enero de 2007, invitó a Costa Rica a adherirse al Convenio sobre la Ciberdelincuencia hecho en Budapest, el 23 de noviembre de 2001, de conformidad con su artículo 37.

Este instrumento jurídico entró en vigencia el 1 de julio de 2004 como fruto de la reunión internacional de expertos celebrada en Budapest, Hungría, en noviembre de 2001. En la actualidad, son Partes de este Convenio los siguientes miembros del Consejo de Europa: Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Alemania, Hungría, Islandia, Italia, Letonia, Lituania, Malta, Moldavia, Montenegro, Reino de los Países Bajos, Noruega, Portugal, Rumania, Serbia, Eslovaquia, España, Eslovenia, Antigua República Yugoslava de Macedonia, Suiza, Ucrania y Reino Unido. Asimismo, como Parte de este Convenio, aparece los Estados Unidos de América, el cual no es miembro del Consejo de Europa.

Su texto es considerado como el estándar mundial en esta materia, lo que ha cerrado la posibilidad de que se elabore un Convenio Interamericano sobre Delitos Informáticos, como se sugirió en sendas reuniones americanas en México de 2004 y Paraguay en 2009.

Según lo expuso, la Procuraduría General de la República, mediante la opinión jurídica OJ-057-2006 del 24 de abril de 2006, desde la adopción del citado Convenio, diversos países europeos no miembros de la Comunidad Económica, así como otras naciones no europeas, entre estos, Estados Unidos, Japón, Canadá y Sudáfrica vieron con interés el contenido del Convenio sobre la Ciberdelincuencia, en virtud de que representaba una oportunidad valiosa para lograr consenso internacional en la persecución de las nuevas formas de delincuencia ejecutadas a través de los medios telemáticos. Los países mencionados son los que han suscrito el Acuerdo fuera de la Unión Europea, con miras a incorporarlo a su legislación interna, mientras que en América Latina, Argentina, México Chile, República Dominicana y Costa Rica han sido invitados a formar parte de dicho Convenio. Cabe recalcar que, a la fecha, ningún país latinoamericano es Parte de dicho instrumento jurídico.

Con la intención que los demás países de la región conozcan e integren a su legislación interna el texto del Convenio, o que al menos elaboren legislación sobre ciberdelitos que cumplan con los términos del acuerdo europeo, la Organización de Estados Americanos ha realizado numerosas reuniones con sus países miembros, procurando encontrar respuestas conjuntas para enfrentar conductas que las más de las veces no encuentran reacción en los ordenamientos jurídicos penales latinoamericanos, o se encuentran mal reguladas, como es el caso de Costa Rica. Este vacío o inexistencia normativa se explica no por negligencia o desinterés del legislador, sino principalmente por el avance tan acelerado de las tecnologías de información y comunicación que dejan rezagadas las previsiones penales en cuanto a conductas sancionables. Ello es, pues, una consecuencia lógica de un fenómeno mundial al que el Derecho positivo apenas está comenzando a dar respuestas adecuadas. Si bien el tema de los delitos informáticos es aún una materia jurídicamente novedosa y de poco desarrollo doctrinal, hemos encontrado que en Costa Rica la legislación penal (no solo la que contempla el propio Código Penal, sino otras leyes especiales que contiene tipos penales informáticos) no mantiene un contenido adecuado para perseguir, prevenir o reprender las conductas lesivas de los delincuentes informáticos. Más aún, el propio legislador nacional ha cometido yerros importantes a la hora de elaborar y emitir tipos penales, pues no solo ha promulgado normas que bien podrían tenerse por contradictorias, sino que ha suprimido inexplicablemente algunas de las pocas existentes. Si bien no analizaremos a fondo las normas penales existentes en Costa Rica, sí es necesario hacer al menos mención de estas importantes deficiencias legislativas para apoyar la posición de reelaborar las normas penales existentes en la materia, y ajustarlas en particular al Convenio sobre la Ciberdelincuencia, consecuencia obligada de ser Parte de este instrumento jurídico Internacional.

En el año 2000, los países miembros de la Organización de Estados Americanos (OEA), en una reunión en Costa Rica, decidieron optar por la elaboración de “leyes-tipo” para que fuesen aplicables a los países participantes en el evento. Desde ese momento, la representación de Costa Rica propuso más bien la elaboración de un Convenio Interamericano sobre Delitos Informáticos, por las enormes ventajas que representa la normativa supranacional.

Posteriormente, a finales de enero y principios de febrero de 2004, en el Foro Legislativo en Materia de Delitos Cibernéticos, celebrado en la Ciudad de México y organizado por la Organización de Estados Americanos, el Departamento de Estado y la Secretaría de Justicia del Gobierno de los Estados Unidos, se evaluó el desarrollo de la normativa latinoamericana en la materia, llegando a la conclusión de que el tema de la ciberdelincuencia tenía poco o ningún avance en las legislaciones del continente, salvo contadas excepciones.

En ese foro de conocimiento una vez más se reiteró la necesidad de que los países integrantes del continente americano contasen con un convenio internacional sobre delitos informáticos, tomando en cuenta, entre otros motivos, el fracaso de la solución de leyes-tipo en materia represiva que se quiso implantar en

el pasado como solución para las diferentes naciones participantes que deseaban actualizar su legislación. Muestra de ello es que aún existen numerosos países que carecen absolutamente de leyes sobre delitos informáticos, tales como algunos países centroamericanos (Nicaragua o Guatemala), y otros que las tienen de manera deficiente o insuficiente, como Chile, Paraguay o Costa Rica. En ese mismo Foro, además, se presentó por primera vez a los países participantes el Convenio sobre la Ciberdelincuencia, en el marco del Consejo de Europa. Precisamente, una de las conclusiones a las que se llegó era la posibilidad de ser parte del presente Convenio y pensar en la posibilidad de elaborar, posteriormente, un tratado propiamente del continente americano en tan importante temática. No obstante, la posibilidad de elaborar un convenio americano en materia de delitos informáticos no pareció viable, pues cuando tal idea se planteó una vez más en el foro sobre Ciberdelincuencia llevado a cabo en Paraguay en el año 2009, la representación de los Estados Unidos de América la objetó bajo el argumento de que ya existía un Convenio Internacional sobre la materia, precisamente, el Convenio en examen, del cual nuestro país debería ser Parte.

La utilización de un cuerpo normativo como este Convenio ofrece mayores garantías de cumplimiento que las que posee, por ejemplo, las “leyes-modelo” o “leyes-tipo”, dado que, por su naturaleza, el convenio tiene un rango superior al de las normas comunes, situación que exigiría reformar la normativa nacional que no se adecue a los términos del presente tratado. Además, este instrumento internacional tiene una aplicación territorial tan amplia como países sean Partes.

Cabe indicar que, precisamente por la extensa cantidad de redes de cómputo dentro y fuera de los países, así como la incursión de la Internet, nos enfrentamos a un serio problema de territorialidad que solo puede verse solventado con la aplicación de acuerdos internacionales y la adopción de medidas técnicas uniformes en los diferentes territorios donde se pretenda perseguir penalmente a los infractores cibernéticos. Consideramos que cualquier convenio internacional que pretenda dar soluciones globales debe contemplar en su contenido la posibilidad de tener el territorio de sus miembros como uno solo, y reprimir las conductas delictivas efectuadas fuera de sus fronteras con la misma energía como si el hecho hubiese ocurrido en su propio territorio, tal como ya ocurre con los acuerdos internacionales sobre drogas o el Protocolo al Convenio sobre Derechos del Niño, los cuales contemplan tal posibilidad y constituyen una excelente herramienta en la lucha contra la impunidad.

Resulta de interés público que el Estado costarricense preste atención y procure suscribir convenios internacionales sobre temas que traten de problemáticas jurídicas y situaciones que involucren la aplicación de herramientas tecnológicas, ya de por sí de urgente corrección en nuestro país. La rama de las comunicaciones es sin duda alguna el campo donde el desarrollo tecnológico actual ha tenido su mayor expresión y ello se evidencia en las múltiples opciones con que cuenta el ciudadano para realizar sus contactos, la velocidad, prontitud y

seguridad con que puede ejecutarlas, y la constancia de los sistemas remotos, en tanto servicios públicos.

Como consecuencia de esas facilidades, aunado al fenómeno mundial de la Internet, como medio de comunicación por excelencia que engloba a su vez otras posibilidades de comunicación muy diferentes de las tradicionales, la actividad académica e informativa original ha dado paso a una enorme afluencia de tipo más comercial y financiero que provocó en pocos años una nueva forma de relacionarse entre las personas, independientemente del idioma, territorio, estrato social o nivel cultural de ellas.

En el caso concreto de los delitos informáticos, los cuales constituyen la cara oculta y la aplicación torcida de las ventajas tecnológicas, donde personas inescrupulosas aprovechan los enormes beneficios de las telecomunicaciones para llevar a cabo actos condenables y que, increíblemente, pueden quedar sin sanción en virtud de la ausencia de normas penales claras o inteligibles que a fin de cuentas resultan de difícil o imposible aplicación por el juez. Así, por ejemplo, en Costa Rica ciertas conductas no se encuentran tipificadas, tales como el espionaje informático, el phishing, pharming, la suplantación de personalidad, la protección de datos personales, difusión de virus, suplantación de páginas o sitios Web, al igual que la facilitación del nombre de usuario y clave de acceso a sistemas públicos (las cuales solo se dan en legislación aduanera y tributaria).

De allí la urgencia de echar mano de las posibles soluciones que brinde el derecho positivo penal para lograr prevenir y sancionar estas lamentables conductas.

La aprobación del Convenio sobre la Ciberdelincuencia tendrá como consecuencia principal el remozamiento de la legislación penal costarricense que intenta regular el tema, lo cual vendrá a mejorar los términos y conceptos en que están redactados los tipos penales, y a crear nuevas figuras que aún no encuentran debida regulación en las normas represivas. Sin perder de vista que se trata de materias aún muy novedosas y de poco desarrollo doctrinal, hemos encontrado que en Costa Rica la legislación penal (no solo la que contempla el propio Código Penal, sino otras leyes especiales que contienen tipos penales informáticos, según mencionaremos) no mantiene un contenido adecuado para perseguir, prevenir o reprender las conductas lesivas de los delincuentes informáticos. Cabe destacar que la legislación nacional contiene normas que bien podrían tenerse por contradictorias y además se han suprimido temporalmente algunas de las pocas figuras penales existentes.

El análisis del presente Convenio justifica la necesidad de que Costa Rica deba aprobarlo con prontitud, procediendo en lo posible a llevar a cabo importantes reformas legislativas en la materia, dada la necesidad de crear nuevas figuras que respondan a las necesidades sociales producidas por la incorporación de las nuevas tecnologías de información y comunicación en nuestro medio. En

este sentido, también resulta de urgente aprobación el proyecto de ley sobre delitos informáticos, tramitado bajo el expediente N.º 17.613.

El Convenio sobre la Ciberdelincuencia contiene elementos novedosos. Por ejemplo, crea dos nuevos bienes jurídicos tutelados, como son la protección de la información en soportes digitales y el funcionamiento de un sistema informático. Además, invita a crear tipos penales donde se sancione a personas jurídicas, corriente de pensamiento que tiene un buen nivel de aceptación entre los estudiosos de la materia.

En su contenido, el artículo 1 del Convenio incorpora cuatro definiciones, sobre los que se entenderá por "sistema informático", "datos informáticos", "proveedor de servicios" y "datos sobre el tráfico". Si bien no se incluye el concepto de "sistema de información", sino que se limita a los sistemas informáticos, esto es, las redes o conexión lógica entre computadoras, en cualquier tipo de plataforma, ello no obsta para que nuestro legislador, en su momento, incluya correctamente ambos tipos de sistemas dentro de la protección normativa, pues no se trata de los mismos conceptos, sino que cada uno de ellos tiene aplicaciones diferentes, sin guardar siquiera relación de jerarquía o de género a especie.

La única norma que define los "datos sobre el tráfico" es el artículo 5 del decreto ejecutivo N.º 35205 de 16 de abril de 2009, denominado Medidas de Protección de la Privacidad en las Telecomunicaciones, pero no es exactamente materia penal ni ha sido elaborada para fines de delitos informáticos. Con miras a lograr un nivel normativo equivalente dentro de los territorios de los Estados Parte de este, el Convenio sobre la Ciberdelincuencia contempla una serie de disposiciones que procuran uniformar los tipos penales en los diferentes Ordenamientos Jurídicos. Tales disposiciones se refieren a las conductas que deben tenerse como punibles en cada país, relacionadas con la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos.

Así por ejemplo, el artículo 2 del Convenio se refiere al acceso no autorizado a sistemas informáticos. El artículo 196 bis del Código Penal, Ley N.º 4573 de 4 de mayo de 1970 se refiere a la violación de las comunicaciones electrónicas, con un contenido amplio que procura abarcar cualquier conducta que lesione las comunicaciones íntimas de los ciudadanos. No obstante, en ese tipo penal no se entiende a qué se refiere con soportes electrónicos, informáticos o telemáticos. El único soporte que tiene sentido real es el soporte magnético. Inexplicablemente se omite la referencia a los soportes ópticos. Por tanto, debería incluirse también en la norma punitiva.

El artículo 3 regula la interceptación dolosa y sin autorización, utilizando medios técnicos, de datos en un sistema informático o de transmisiones no públicas. La totalidad de los conceptos que abarca este numeral no se hayan recogidas íntegramente en la legislación costarricense, pues los tipos penales

contemplados en la legislación nacional se refieren exclusivamente a materia tributaria y aduanera, no aplicándose a otros casos similares.

No obstante, el citado artículo 196 bis del Código Penal sanciona la interceptación o interferencia de datos y otros elementos si son llevados a cabo sin consentimiento del titular de ellos, o si se hace con la intención de vulnerar la intimidad o secretos del afectado. Remitimos a este nuevamente para corroborar la existencia de los verbos "interceptar" e "interferir" y "desviar de su destino", en referencia a mensaje, datos e imágenes contenidas en cualquier tipo de soporte, sea este electrónico, informático, magnético o telemático. No obstante que dicho artículo no se describe de la misma forma que la contemplada en el presente Convenio, aunque su contenido sí parece llenar los requisitos que se exigen en el cuerpo normativo internacional. Por su parte, el artículo 229 bis del Código Penal castiga igualmente el acceso sin autorización a los datos registrados en una computadora: Se reitera la conclusión anterior en el tanto las acciones sancionadas en dichos tipos penales parecen sujetarse a las exigencias de este Convenio.

Por lo tanto, en principio, no se requeriría adicionar más verbos activos, aunque igualmente ello puede ser objeto de revisión, especialmente porque la forma en que están redactadas ciertas conductas podría ser reiterativa, especialmente en lo que se refiere a la acción de borrar datos, contemplada en ambos tipos penales, y con la única diferencia de que en el primer caso la intención debe ser "descubrir los secretos o vulnerar la intimidad de otro"; mientras que en el segundo tipo penal simplemente se exige "falta de autorización", aunque las conductas sean idénticas. Ello ha procurado corregirse en el nuevo proyecto de ley sobre la materia, expediente N.º 17.613.

El artículo 4 del Convenio se refiere a la interferencia en los datos, consistente en conductas que causen daños, borren, deterioren, alteren o supriman datos informáticos, provocando daños graves. El artículo 229 bis de nuestro Código Penal, citado en el punto anterior, contiene los verbos "borrar", "suprimir", "modificar" e "inutilizar", sin autorización, los datos registrados en una computadora, por lo que creemos que esta figura se halla debidamente contemplada en nuestra legislación punitiva.

A pesar de lo indicado, pensamos que su redacción podría precisarse aún más, pues su contenido es sumamente genérico. Tomemos en cuenta que no todos los "datos" que se encuentran en una computadora tienen el mismo valor. Quizás debería pormenorizarse según los medios empleados para el borrado, supresión, etc., si es efectuado mediante el empleo de programas dañinos, tales como virus, gusanos, programación, empleo de programas destinados para ello, choque electromagnéticos, etc. Recordemos que los sistemas operativos tienen el borrado y destrucción de datos como una de sus funciones normales, y no todos los elementos eliminados guardan el mismo nivel de importancia, esto es, no es lo mismo eliminar el archivo *command.com* que los registros de la papelera de reciclaje o los mensajes electrónicos borrados.

En el mismo sentido del numeral anteriormente citado, el artículo 111 de la Ley de Administración Financiera de la República y Presupuestos Públicos N.° 8131 de 18 de setiembre de 2001 señala las sanciones contra funcionarios públicos o personas particulares que causen daños a sistemas informáticos de la administración financiera y de proveeduría de las instituciones públicas. Nótese que la existencia de este artículo es innecesaria pues el sujeto activo puede ser cualquier persona, sean funcionarios públicos o particulares.

Además, su redacción carece de técnica legislativa, es confusa y reiterativa, pues sus verbos activos ya se encuentran contemplados en los tipos que recoge el Código Penal, según hemos citado.

El artículo 5 del Convenio se refiere a la interferencia en el sistema, descrito como una obstaculización grave, dolosa e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daños, borrado, deterioro, alteración o supresión de datos informáticos. Una vez más citamos el artículo 229 bis el cual, en sus párrafos finales, contempla sanciones en caso de que, con ocasión de la alteración de datos o sabotaje informático, se entorpeciese o inutilizase una base de datos o sistema informático. Por demás, el mismo artículo, en su párrafo final, dispone la penalización según el resultado lesivo de la conducta.

Por su parte el artículo 6 se refiere al abuso de los dispositivos, sancionando la tenencia, producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de programas de cómputo o similares que sirvan para el acceso, intercepción, interferencia de datos o de sistemas informáticos, incluyendo la destrucción, inutilización, alteración, etc., o bien, contraseñas, códigos de entrada o datos informáticos o similares que permitan acceder a un sistema informático. En el caso de la creación o tenencia de tales dispositivos, el propio Convenio prevé la posibilidad de que se exima de responsabilidad la conducta si los programas de cómputo no han sido creados originalmente para fines ilícitos.

La legislación costarricense contiene una disposición similar, concretamente en la Ley de Procedimiento de Observancia de Derechos de Propiedad Intelectual, artículos 2 bis, 62 y 62 bis. No obstante, sí se hace necesaria la creación legislativa expresa de figuras penales más precisas y que su contenido tenga alcances generales.

Más aún, el delito denominado “suplantación de personalidad” tampoco se encuentra contemplado en la legislación nacional, en cuanto al uso ilegítimo de nombres de usuario y claves de acceso para acceder a sistemas de información. En realidad, disposiciones que penan tal conducta se encuentran previstas solamente en materia aduanera y tributaria.

El artículo 7 del Convenio contempla un delito informático de gran relevancia, como es la falsificación informática, lo que incluye la introducción,

alteración, borrado o supresión de datos informáticos con la intención de que se tengan como auténticos para cualquier efecto legal. Si bien existe un tipo penal que sanciona el fraude informático, artículo 217 bis del Código respectivo, existe discordancia en la denominación de la norma, pues el Convenio en examen denomina a dichas conductas como "falsificación informática" mientras que en el Código Penal de Costa Rica se le llama "Fraude Informático". Si bien los términos de este artículo del Código Penal costarricense son bastante criticables, al no incluir los componentes de entrada ni hacer énfasis en la noción del concepto básico de "sistema" (entrada, procesamiento, salida), sí parece cumplir, al menos, con el requisito exigido en el Convenio europeo. No obstante, de la redacción, bastante criticable, parece exigirse que el resultado del hecho delictivo se produzca en el procesamiento (caja negra) del sistema, y no en su salida, lo que exige una revisión y reelaboración del tipo penal.

Por su parte el artículo 8, establece la figura del fraude informático, el cual consiste en la introducción, alteración, borrado o supresión de datos informáticos, o la interferencia en el funcionamiento de un sistema informático, con el objeto de obtener ilícitamente un beneficio económico ilegítimo para sí o para un tercero.

Otro aspecto de gran relevancia lo constituye el artículo 9 del Convenio, referido a los delitos relacionados con la pornografía infantil, incluyendo cualquier conducta que lleve a la producción, oferta, puesta a disposición, difusión, transmisión, adquisición o posesión de pornografía infantil en un sistema informático o soporte apropiado para almacenar datos informáticos. La calidad y cantidad de normas jurídicas que protegen a los y las menores en Costa Rica ha recibido reconocimiento del propio Consejo de Europa, por lo que es posible afirmar que nuestro país cumple debidamente con la exigencia del numeral 9 del Convenio sobre Ciberdelincuencia. Además, la posesión de pornografía infantil es penalizada mediante el artículo 173 bis del Código Penal. Costa Rica ha procurado mantener una actitud de salvaguarda de los derechos de los menores, protegiendo precisamente la indemnidad e inexperiencia sexual de los potenciales afectados.

El artículo 16, referido a la conservación rápida de datos informáticos almacenados, tampoco encuentra legislación precisa en materia procesal penal, que trate expresamente de la conservación de datos informáticos. De hecho, no existe norma alguna que obligue de oficio a los denominados ISP's o proveedores de servicios de Internet a conservar algún dato almacenado por sus usuarios. La única manera como ello podría ocurrir es en virtud de una orden judicial, emanada por juez competente dentro del marco de una investigación abierta.

Otros aspectos contemplados en el presente Convenio de especial relevancia, convienen ser destacados, tales como la cooperación internacional entre los Estados Parte, a los fines de las investigaciones o procedimientos concernientes a infracciones penales relacionadas con sistemas cómputo y datos, o para la recolección de pruebas, en formato electrónico de una infracción penal.

Asimismo, se establecen ciertas reglas relacionadas con la extradición y la asistencia mutua entre Estados Parte, específicamente en materia de adopción de medidas cautelares y los poderes de investigación, incluyendo la posibilidad de que una parte solicite a otra parte que registre o acceda, confisque y revele datos almacenados por medio de un sistema informático, así como acceso transfronterizo a datos almacenados y obtención en tiempo real de datos sobre el registro, mecanismos que son de gran utilidad tratándose de actividades que generalmente trascienden las fronteras, resultando clave la cooperación y asistencia mutua entre Estados.

Finalmente, conviene destacar que el Convenio admite reservas de los países, en caso de que alguna disposición contradiga los términos de la Constitución Política.

Señores Diputados, como puede apreciarse, la adhesión de Costa Rica a este Convenio es de suma importancia pues vendría a complementar las acciones legislativas emprendidas en materia de delitos informáticos (dentro del proyecto N.º 17.613) y complementariamente puede incidir en el tema de protección de la niñez, en todos sus extremos y constituye una clara señal a la comunidad internacional del compromiso de Costa Rica por reprimir estas conductas que aún no encuentran una respuesta punitiva adecuada en nuestro Ordenamiento Jurídico.

En virtud de lo anterior, sometemos a conocimiento, y aprobación de la Asamblea Legislativa, el proyecto de ley adjunto relativo a la **"APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA".**

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

"APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA"

ARTÍCULO ÚNICO.- Apruébese, en cada una de sus partes, el **"CONVENIO SOBRE LA CIBERDELINCUENCIA"**, hecho en Budapest el 23 de noviembre de 2001**",** cuyo texto es el siguiente:

YO, KATIA MARÍA JIMÉNEZ POCHET, TRADUCTORA OFICIAL DEL MINISTERIO DE RELACIONES EXTERIORES Y CULTO DE LA REPUBLICA DE COSTA RICA, NOMBRADA POR ACUERDO NUMERO 8-DJ DEL 21 DE NOVIEMBRE DEL 2000 PUBLICADO EN LA GACETA NUMERO 45 DEL 5 DE MARZO DE 2001, CERTIFICO QUE LA TRADUCCIÓN DEL IDIOMA INGLÉS AL IDIOMA ESPAÑOL DEL SIGUIENTE DOCUMENTO DICE LO SIGUIENTE:

Convenio sobre la Ciberdelincuencia ----------

[Budapest, 23.XI. 2001] ----------

Preámbulo----------

Cada Parte miembros del Consejo de Europa y los otros Estados signatarios del presente Convenio, ----------

---

Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros; ----------

---

Reconociendo el interés de intensificar la cooperación con Cada Parte parte en el presente Convenio; ----------

---

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común destinada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación apropiada y el fomento de la cooperación internacional; ----------

---

Conscientes de los profundos cambios suscitados por la digitalización, la convergencia y la globalización continua de las redes informáticas;----------

---

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de esas redes; ----------

---

Reconociendo la necesidad de una cooperación entre Cada Parte y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información; ----------

---

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;----------

---

Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los

sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;----------

---

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966), y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el derecho al respeto a la intimidad; ----------

---

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales; ----------

---

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de menores (1999); ----------

---

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre Cada Parte miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos; ----------

---

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8; ----------

---

Recordando las recomendaciones del Comité de Ministros N.º (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, N.º R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, N.º R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, N.º R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de

telecomunicación, con especial referencia a los servicios telefónicos, así como N.º R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de delitos informáticos, y N.º R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información; ----------

Teniendo en cuenta la Resolución N.º 1, adoptada por los Ministros europeos de Justicia, en su XXI Conferencia (Praga, 10 y 11 de junio 1997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución N.º 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser partes en el Convenio, y reconocía la necesidad de disponer de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciberdelincuencia; ----------

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa; ----------

Han convenido lo siguiente: ----------

Capítulo I. Terminología ----------

Artículo 1. Definiciones ----------

A los efectos del presente Convenio, ----------

a) por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan en ejecución de un programa; ----------

b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función; ----------

c) por «proveedor de servicios» se entenderá: ----------

i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático; y ----------

ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio; ----------

---

d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.----------

---

Capítulo II. Medidas que deberán adoptarse a nivel nacional ----------

---

Sección 1. Derecho penal sustantivo----------

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos----------

---

Artículo 2. Acceso ilícito----------

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, el acceso deliberado e ilegítimo a la totalidad o una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.----------

---

Artículo 3. Interceptación ilícita ----------

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.-----

---

Artículo 4. Interferencia en los datos ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.----------
2. Cualquier Estado Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado I provoquen daños graves.----------

Artículo 5. Interferencia en el sistema ----------

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.----------

Artículo 6. Abuso de los dispositivos ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos: ----------

   a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:----------

      i. un dispositivo, incluido un programa informático adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; ----
      ii. una contraseña, un código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las delitos previstas en los artículos 2 a 5; y

   b. la posesión de alguno de los elementos contemplados en los apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un determinado número de dichos elementos para que se considere que existe responsabilidad penal.----------

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo, no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del

presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.----------

3. Cualquier Parte podrá reservarse el derecho de no aplicar lo dispuesto en el el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, distribución o cualquier otras puesta a disposición de los elementos indicados en el apartado 1.a.ii del presente artículo.----------

Título 2. Delitos informáticos----------

Artículo 7. Falsificación informática----------

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean directamente legibles e inteligibles. Cualquier parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.----------

Artículo 8. Fraude informático----------

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: ----------

a. cualquier introducción, alteración, borrado o supresión de datos informáticos; ----------

b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.----------

Título 3. Delitos relacionados con el contenido----------

Artículo 9. Delitos relacionados con la pornografía infantil ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos: ----------

    a. la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; ----------

b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; ----------
c. la difusión o transmisión de pornografía infantil por medio de un sistema informático; ----------
d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;----------
e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.----------

2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:
a. un menor comportándose de una forma sexualmente explícita; --------
b. una persona que parezca un menor comportándose de una forma sexualmente explícita;----------
c. imágenes realistas que representen un menor comportándose de una forma sexualmente explícita.----------
---

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.----------
---

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.-----
---

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines----------
---

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines----------
---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, las infracciones de la propiedad intelectual, según se definen en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París del 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Propiedad Intelectual, a excepción de cualquier derecho moral otorgado por dichos convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. ----------
---

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, las infracciones de los derechos afines definidos por la legislación de dicha

Parte, de conformidad con las obligaciones que ésta haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

---

3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.----------

---

Título 5. Otras formas de responsabilidad y de sanciones ----------

---

Artículo 11. Tentativa y complicidad ----------

---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previsto de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.----------

---

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cualquier tentativa de comisión de alguno de los delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a y c. del presente Convenio, cuando dicha tentativa sea intencionada.----------

---

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.----------

---

Artículo 12. Responsabilidad de las personas jurídicas ----------

--- ---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas, por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de: ----------

---

a. un poder de representación de la persona jurídica; ----------
b. una autorización para tomar decisiones en nombre de la persona jurídica; ----------
c. una autorización para ejercer funciones de control en la persona jurídica.----------

---

2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.----------

---

3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de la persona jurídica podrá ser penal, civil o administrativa. ----------

---

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.----------

---

Artículo 13. Sanciones y medidas ----------

---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en los artículos 2 al 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad. ----------

---

2. Cada Parte garantizará la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12. ----------

---

Sección 2. Derecho procesal ----------

Título 1. Disposiciones comunes----------

Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento

---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente sección para los fines de investigaciones o procedimientos penales específicos.----------

---

2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:----------

---

a. los delitos penales previstos de conformidad con los artículos 2 a 11 del presente Convenio; ----------
b. otros delitos cometidos por medio de un sistema informático; y --------
c. la obtención de pruebas electrónicas de un delito.----------

---

3.

a. Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.----------

---

b. Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios: ----------

---

i. utilizado en beneficio de un grupo restringido de usuarios, y----

---

ii. no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.----------

---

Artículo 15. Condiciones y salvaguardas. ----------

----- ----------

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950) , del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) y de otros instrumentos internacionales aplicables en materia

de derechos humanos, y que deberá integrar el principio de proporcionalidad.----------

2. Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros, aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate----------

3. Siempre que sea conforme con el interés particular, con la correcta administración de la justicia , cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.----------

Título 2. Conservación rápida de datos informáticos almacenados----------

Artículo 16. Conservación rápida de datos informáticos almacenados----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación. ----------

2. Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentran en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables. ----------

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto por su derecho interno.--

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.----------

---

Artículo 17. Conservación y revelación parcial rápidas de datos sobre el tráfico----------

1. Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:----------
   a. para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y---
   b. para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.----------
2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.----------

Título 3. Orden de presentación----------

Artículo 18. Orden de presentación ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar: ----------
   a. a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y----------
   b. a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte, que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.----------
2. Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.----------
3. A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:----------

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio; ----------
---

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios; ----------
---

c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.----------
---

Título 4. Registro y confiscación de datos informáticos almacenados ----------
---

Artículo 19. Registro y confiscación de datos informáticos almacenados------
---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:----------
---

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y ----------

b. a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos en su territorio.----------
---

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades pueden ampliar rápidamente el registro o la forma de acceso similar al otro sistema.----------
---

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:----------
---

a. confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;----------
---

b. realizar y conservar una copia de dichos datos informáticos;----------

---

c. preservar la integridad de los datos informáticos almacenados de que se trate; ----------

---

d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.----------

---

4. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.-
---
---

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a los artículos 14 y 15.----------
---

Título 5. Obtención en tiempo real de datos informáticos----------
---

Artículo 20. Obtención en tiempo real de datos de tráfico----------
---

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:----------
---

a. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y ----------
---

b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:----------

i. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o----------
ii. a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.----------

---

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1 .a), podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.----------
---

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poder artículo, así como toda información al respecto.----------

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21. Interceptación de datos sobre el contenido ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

---

a. a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio; y----------

---

b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica----------

---

i. a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o ----------

---

ii. a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

---

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.----------

---

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquier de los poderes previstos en el presente artículo, así como toda información al respecto.----------

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.----------

---

Sección 3. Jurisdicción----------

Artículo 22. Jurisdicción ----------

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido: ----------

   a. en su territorio; o ----------
   b. a bordo de un buque que enarbole pabellón de dicha Parte; o----------
   c. a bordo de una aeronave matriculada según las leyes de dicha Parte; o ----------
   d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en que se cometió o si ningún Estado tiene jurisdicción territorial respecto del mismo.----------

2. Cualquier Estado podrá reservarse el derecho a no aplicar, o a aplicar únicamente en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b a 1.d del presente artículo o en cualquiera otra parte de los mismos.----------

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su atribuirse la jurisdicción respecto de los delitos mencionados en el artículo 24, apartado 1 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.----------

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.----------

5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.----------

Capítulo III. Cooperación internacional----------

Sección 1- Principios generales----------

Título 1- Principios generales relativos a la cooperación internacional----------

Artículo 23. Principios generales relativos a la cooperación internacional

---

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigación o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos. ----------

---

Título 2. Principios relativos a la extradición----------

Artículo 24. Extradición ----------

---

1. ----------

a. El presente artículo se aplicará a la extradición entre las Partes por los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave. ---------

---

b. Cuando deba aplicarse una pena mínima diferente, en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado.----------

---

2. Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

---

3. Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo. ----------

---

---

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.----------

---

5. La extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición. ----------

---

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo, únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto –a petición de la Parte requirente—a sus autoridades competentes para los fines de las actuaciones penales pertinentes e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable de conformidad con la legislación de dicha Parte. ----------

---

7. ----------

a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado. ----------

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará la exactitud de los datos que figuren en el registro. ----------

---

Título 3- Principios generales relativos a la asistencia mutua ----------

---

Artículo 25. Principios generales relativos a la asistencia mutua ----------

---

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones y procedimientos relativos a delitos relacionados a sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.----------

---

2. Cada Parte adoptará también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículos 27 a 35. ----------

---

3. En caso de emergencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación incluidos el fax y el correo electrónico, en la medida en que dicho medios ofrezcan niveles adecuados de seguridad y de autenticación (incluido el cifrado o encriptación en caso necesario) con confirmación oficial posterior si la Parte requerida lo exige. La Parte

requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.----------

---

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11, únicamente porque la solicitud se refiere a un delito que considere de naturaleza fiscal. ----------

---

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia, constituya un delito en virtud de su derecho interno con independencia que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente. ----------

---

Artículo 26. Información espontánea ----------

---

1. Dentro de los límites de su derecho interno y sin petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podrá ayudar a la parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio, o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo. ----------

---

2. Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello, debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas. ----------

---

Título 4.- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables ----------

---

Artículo 27.- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables ----------

1. Cuando entre las Partes requirentes y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 al 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las partes interesadas convengan en aplicar en su lugar la totalidad o parte, del resto del presente artículo.----------

2. ----------

   a. Cada Parte designará una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución. ----------

   b. Las autoridades centrales se comunicarán directamente entre sí.

   c. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicar al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado. ----------

   d. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro. ----------

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida. ----------

4. Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si: -

   a. la solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político; ----------

   b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales. ----------

5. La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades. ----------

---

6. Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias. ----------

---

7. La Parte requerida informar··sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa. ----------

---

8. La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud. ----------

9. ----------

   a. En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente. ----------

   b. Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL). ----------

   c. Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.----------

   d. Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida. ----------

   e. En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central. ----------

---

Artículo 28 - Confidencialidad y restricción de la utilización ----------

1. En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo. ----------

---

2. La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que: ----------

---

   a. se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o ----------

---

   b. no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud. ----------

---

3. Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informar·de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedar· vinculada por ella.

---

4. Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material. ----------

---

Sección 2 - Disposiciones especiales ----------

Título 1 - Asistencia mutua en materia de medidas provisionales ----------

---

Artículo 29 - Conservación rápida de datos informáticos almacenados ---------

---

1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

---

2. En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará: ----------

a. a la autoridad que solicita dicha conservación; ----------
b. el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo; ----------
c. los datos informáticos almacenados que deben conservarse y su relación con el delito; ----------
d. cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;----------
e. la necesidad de la conservación; y ----------
f. que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados. ----------

---

3. Tras recibir la solicitud de otra Parte, la Parte requerida tomar· las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación. ----------

---

4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación. ----------

---

5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si:
a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político; ----------
b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales. ----------

---

6. Cuando la Parte requerida considere que la conservación por sí sola no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informar· de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud. ----------

---

7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de

registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma. ----------

Artículo 30 - Revelación rápida de datos conservados sobre el tráfico----------

1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelar· rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación. -----
2. La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si: ----------
   a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;
   b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales. ----------

Título 2 - Asistencia mutua en relación con los poderes de investigación----------

Artículo 31 - Asistencia mutua en relación con el acceso a datos informáticos almacenados ----------

1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29. -----
2. La Parte requerida dar· respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo. ----------
3. Se dará respuesta lo antes posible a la solicitud cuando: ----------
   a. existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o ----------
   b. los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida. ----------

Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público----------
---

Una Parte podrá, sin la autorización de otra Parte: ----------

a. tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o ----------

b. tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.----------

---

Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico----------

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regir· por las condiciones y procedimientos establecidos en el derecho interno. ----------

---

2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país. ----------

---

Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido ----------

---

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables. ----------

Título 3 - Red 24/7 ----------

Artículo 35 - Red 24/7 ----------

---

1. Cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas: ----------

---

a. el asesoramiento técnico; ----------
b. la conservación de datos en aplicación de los artículos 29 y 30; -------
c. la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos. ----------
---

---

2. ---
a. El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente. ----------
b. Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente. ----------
---

3. Cada Parte garantizará la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red. ----------

---

Capítulo IV - Disposiciones finales ----------

Artículo 36 - Firma y entrada en vigor ----------

---

1. El presente Convenio estará abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración. ----------

---

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa. ----------

---

3. El presente Convenio entrar· en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2. ----------

---

4. Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2. ----------

---

Artículo 37 - Adhesión al Convenio----------

1. Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá· invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros. ----------

2. Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrar· en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa. ----------

Artículo 38 - Aplicación territorial ----------

1. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá· especificar el territorio o territorios a los que se aplicará el presente Convenio. ----------

2. En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrar· en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración. ---

3. Toda declaración formulada en virtud de los dos apartados anteriores podrá retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación. ----------

Artículo 39 - Efectos del Convenio----------

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:----------
   - el Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE nº 24); ----------

- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº 30); ----------
- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE nº 99). ----------

---

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio. ----------

---

3. Nada de lo dispuesto en el presente Convenio afectar· a otros derechos, restricciones, obligaciones y responsabilidades de las Partes. ----------

---

Artículo 40 - Declaraciones----------

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e). ----------

---

Artículo 41 - Cláusula federal----------

---

1. Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III. ----------

---

2. Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo. ----------

---

3. Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal

informar·de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación. ----------

Artículo 42 - Reservas ----------

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá· declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas. ----------

Artículo 43 - Situación de las reservas y retirada de las mismas----------

1. La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica que la retirada de una reserva surtir· efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior. ----------

2. La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias. ----------

3. El Secretario General del Consejo de Europa podrá· preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva. ----------

Artículo 44 - Enmiendas----------

1. Cualquier Estado Parte podrá· proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37. ----------

2. Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentar· al Comité de Ministros su opinión sobre la enmienda propuesta.----------

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda. ----------

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo será remitido a las Partes para su aceptación. ----------

5. Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrar· en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General. ---------

Artículo 45 - Solución de controversias ----------

1. Se mantendrá informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio. ----------

2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas. ----------

Artículo 46 - Consultas entre las Partes----------

1. Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar: ----------
   a. la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio; ----------
   b. el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico; ----------
   c. el estudio de la conveniencia de ampliar o enmendar el presente Convenio. ----------

2. Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1. ----------

---

3. Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes. ----------

---

4. Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que éstas determinen. ----------

---

5. Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeñar sus funciones en aplicación del presente artículo.

Artículo 47 - Denuncia----------

---

1. Cualquier Parte podrá denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa. ----------

---

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación. ----------

---

Artículo 48 - Notificación----------

El Secretario General del Consejo de Europa notificar· a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo: ----------

a. cualquier firma; ----------
b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión; ----------
c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37; ----------
d. cualquier declaración formulada en virtud del artículo 40 o reserva formulada de conformidad con el artículo 42; ----------
e. cualquier otro acto, notificación o comunicación relativo al presente Convenio. ----------

---

En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio. ----------
---
Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitir copias certificadas a cada uno de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo. ----------
---

ULTIMA LINEA ----------
-------EN FE DE LO CUAL SE EXPIDE LA PRESENTE TRADUCCIÓN OFICIAL DEL INGLÉS AL ESPAÑOL COMPRENSIVA DE TREINTA Y TRES FOLIOS. FIRMO Y SELLO EN LA CIUDAD DE SAN JOSÉ, COSTA RICA AL DÍA DIECINUEVE DE ABRIL DE DOS MIL DOCE. SE ADJUNTAN Y CANCELAN LOS TIMBRES DE LEY Y SE ANULA EL REVERSO DE CADA FOLIO. ----------

REPÚBLICA DE COSTA RICA
MINISTERIO DE RELACIONES EXTERIORES Y CULTO
DIRECCION GENERAL DE POLITICA EXTERIOR

ESTELA BLANCO SOLÍS
DIRECTORA GENERAL A. I. DE POLÍTICA EXTERIOR

CERTIFICA:

Que las anteriores treinta y tres fotocopias, son fieles y exactas de la traducción oficial del idioma inglés al idioma español del texto del Convenio sobre la Ciberdelincuencia, hecho en Budapest, el veintitrés de noviembre de dos mil uno. Se extiende la presente, para los efectos legales correspondientes, en la Dirección General de Política Exterior a las diez horas del nueve de mayo del dos mil doce.

Rige a partir de su publicación.

Dado en la Presidencia de la República, San José, a los tres días del mes de mayo del dos mil doce.

Laura Chinchilla Miranda
PRESIDENTA DE LA REPÚBLICA

J. Enrique Castillo Barrantes
MINISTRO DE RELACIONES EXTERIORES Y CULTO

2 de julio de 2012

Este texto es copia fiel del expediente N.º 18.484. Se respetan literalmente la ortografía, el formato y la puntuación del original, según lo dispuesto por la Sala Constitucional de la Corte Suprema de Justicia en su resolución N.º 2001-01508, de las ocho horas con cincuenta y cuatro minutos de 23 de febrero de 2001.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Permanente Especial de Relaciones Internacionales y de Comercio Exterior.