Convenio sobre la Ciberdelincuencia: Convenio de Budapest

Autor

Verónica Barrios Achavar
Email: vbarrios@bcn.cl
Tel.: (56) 32 226 3179
(56 2) 22701884

Andrea Vargas Cárdenas
Email: avargas@bcn.cl
Tel.: (56) 32 226 3174
(56 2) 22701871

Nº SUP: 116108

Resumen

El Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) es el acuerdo internacional de uso más extendido para desarrollar la legislación de combate al cibercrimen. El tratado ha sido ratificado por 60 Estados, incluidos los Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia y Japón. Chile se incorporó tras la aprobación por parte del Congreso Nacional el 16 de noviembre de 2016. Con posterioridad, el Gobierno chileno, con fecha 21 de abril de 2017, depositó en Estrasburgo, Francia, el instrumento de adhesión al Convenio sobre la Ciberdelincuencia. Tres meses después del depósito, Chile se convirtió en el miembro número 54 del Tratado y el primero en Sudamérica. Durante el presente año el Convenio ha sido ratificado por Argentina y Colombia.

La Convención, en síntesis, tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de estos delitos y establecer un régimen efectivo de cooperación y asistencia internacional. Entre sus principales disposiciones destacan la obligación de tipificar delitos contra la integridad de los sistemas o datos informáticos y su contenido, y establecer procedimientos que faciliten la investigación penal. El Acuerdo resuelve también los aspectos de la cooperación y asistencia internacional en materias como extradición, acceso y consentimiento transfronterizo y el establecimiento de un equipo experto en una Red 24/7 como punto de contacto localizable las 24 horas del día. Existe además un Protocolo Adicional al Convenio sobre la penalización de actos de índole racista y xenófoba.

En Chile, los principales incidentes son actividades relativas al *phishing*, *malware* y el *hackeo* de páginas Web gubernamentales, pero también han aumentado las denuncias de *grooming* y las amenazas contra personas. Nuestro país posee normas como la Ley N°19.223, que tipifica figuras penales relativas a la informática, que resguardan la seguridad del uso de sistemas informáticos, pero en general el sistema legal está desactualizado, o los tipos penales están consagrados para otro delito, y la responsabilidad estatal en términos de protección se encuentra compartida en diferentes organismos.

Introducción

El carácter transnacional de la Ciberdelincuencia ha llevado a adoptar un enfoque normativo de cooperación y armonización regulatoria entre los países para enfrentar la naturaleza global del fenómeno.

Este informe aborda en forma descriptiva las implicancias que el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) ï abierto a la ratificación de otros países- trae aparejado para aquellos Estados que se han hecho parte del tratado, señalando sus objetivos, estado de las ratificaciones, medidas legislativas y de otra índole que los Estados deben adoptar para cooperar en las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos.

La Oficina de Naciones Unidas contra la Droga y el Delito (UNODC, por su sigla en inglés) describió en el año 2013, en su reporte sobre Ciberdelincuencia denominado ñ*Comprehensive Study on Cibercrime*ò que en una sociedad hiperconectada como la de hoy en día, con acceso universal a Internet, casi no existe delito informático e inclusive delito común que no involucre evidencia electrónica ligada a una conexión a Internet, situación que requiere de cambios fundamentales en el enfoque legal, en la recolección de pruebas y en los mecanismos de cooperación internacional para resolver estos asuntos penales (UNODC, 2013).

Entre sus principales hallazgos, el informe enfatiza la fragmentación del marco normativo que regula la Ciberdelincuencia a nivel internacional, lo que refleja la existencia de regímenes con múltiples instrumentos, diferentes temáticas y ámbitos geográficos de aplicación, lo que podría llevar a grupos de países a formar clústeres de cooperación en estas materias, situación que no se ajustaría en forma adecuada a la naturaleza global del cibercrimen (UNODC, 2013: xi).

Al respecto, el estudio señala que a nivel mundial son 82 Estados los que han ratificado algún instrumento internacional de lucha contra el cibercrimen[1], y a partir de una encuesta realizada por el equipo de UNODC el acuerdo multilateral más utilizado para desarrollar la legislación de combate al cibercrimen ha sido el Convenio del Consejo de Europa sobre Ciberdelincuencia (UNODC, 2013: xix).

El presente Informe ha sido elaborado en base al documento ñ*Convenio de Budapest sobre la Ciberdelincuencia y situación de la Ciberseguridad en Chile*ò elaborado en julio de 2016 por la Analista Andrea Vargas.

I. Convenio del Consejo de Europa sobre Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia (*Convention on Cybercrime*), conocido como Convenio de Budapest (COE, Serie Tratados Europeos N° 185), fue suscrito en dicha ciudad el 23 de noviembre de 2001 en el marco de los Estados miembros del Consejo de Europa, y se encuentra en vigor a partir del 1 de julio de 2004.

1. Objetivos

El Convenio de Budapest, según establece su Preámbulo tiene por fin ñincrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos

[1] A saber: *Convention on Cybercrime* (*Council of Europe*), *Convention on Combating Information Technology Offences* (*League of Arab States*), *Agreement on Cooperation in Combating Offences related to Computer Information* (*Commonwealth of Independent States*), *Agreement in the Field of International Information Security* (*Shanghai Cooperation Organization*).

informáticos, así como permitir la obtención de pruebas electrónicas de los delitosò (Consejo de Europa, Preámbulo), mediante ñuna cooperación internacional reforzada, rápida y eficaz en materia penalò(Ibídem).

De acuerdo a su Informe Explicativo, instrumento aprobado en 2001 por el Comité de Ministros del Consejo de Europa y que facilita la aplicación de las disposiciones del Convenio (COE, 2001) , éste tiene por objeto promover la armonización de la legislación que regula el cibercrimen, a nivel del derecho penal sustantivo de cada Parte; mejorar las capacidades nacionales para la investigación de este tipo de delitos, conforme al derecho procesal de cada país; y establecer un régimen ágil y efectivo de cooperación internacional principalmente para facilitar la investigación transnacional de estos delitos (COE, 2001: párr. 16 y Vatis, 2010).

2. Estados Parte

La adhesión al tratado, según establece su Artículo 37°, se encuentra abierta a la incorporación de países que no sean miembros del Consejo de Europa. A la fecha, Budapest ha sido ratificado por 60 Estados, junto a los Estados miembros de la Unión Europea, el Convenio ha sido ratificado por países no europeos , entre ellos Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Colombia. Otras organizaciones internacionales han adherido a él, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT) (COE, *Chart of signatures and ratifications of Treaty* 185).

3. Medidas que deben ser adoptadas por los Estados

El Convenio establece las medidas que deberían ser adoptadas por las Partes, tanto a nivel de derecho penal sustantivo, como en materia de derecho procesal.

Respecto de la jurisdicción de las Partes para conocer y juzgar los delitos (Artículo 22°), cada Estado Miembro deberá adoptar las medidas que la afirmen, cuando el delito se haya cometido: a) en su territorio; o b) a bordo de un buque que enarbole su pabellón; o c) a bordo de una aeronave matriculada según sus leyes; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar de su comisión o si ningún Estado tiene competencia territorial respecto del mismo. Además, el Convenio resuelve en lo que concierne a eventuales conflictos de jurisdicción, cuando varias Partes la reivindiquen respecto de un presunto delito (BCN, 2011).

a. Contenido de derecho penal sustantivo

La Tabla 1 (ver abajo), elaborada Blanca Bórquez (BCN, 2011) sintetiza la tipificación de los delitos de acuerdo al texto del tratado Éste también dispone que deberán ser sancionadas las figuras de tentativa y complicidad en los delitos tipificados (Artículo 11°), y exigir responsabilidad penal a las personas jurídicas (Artículo 12°). Asimismo, el Convenio dispone que las sanciones deberán ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad (Artículo 13°).

b. Contenido de derecho procesal

En materia procesal, el Convenio dispone el compromiso de cada Parte a adoptar las medidas legislativas necesarias para establecer los procedimientos que faciliten la investigación y los procesos penales (Artículo 14°), así como para asegurar la instauración y aplicación de poderes y procedimientos que garanticen la protección de los derechos humanos y las libertades personales (Artículo 15°).

Los procedimientos que la Convención establece se refieren a:

- la conservación rápida de datos informáticos almacenados, incluido el tráfico de datos (Artículo 16°);
- la conservación y revelación parcial rápidas de los datos sobre tráfico (Artículo 17°);
- la orden a personas y proveedores de servicios de presentar la información requerida (Artículo 18°);
- el registro de todo tipo de dispositivo o sistema de almacenamiento informático y la confiscación de los datos informáticos almacenados en ellos (Artículo 19°);
- la obtención en tiempo real de datos relativos al tráfico (Artículo 20°);
- la interceptación de datos relativos al contenido de las comunicaciones (Artículo 21°).

Tabla 1: Conductas que deben tipificarse por el derecho penal sustantivo de cada Estado Parte del Convenio de Budapest

Medidas a nivel nacional: Derecho penal sustantivo. Conductas a tipificar		
Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos	*Acceso ilícito* (Art. 2)	Tipificación del acceso deliberado e ilegítimo a todo o parte de un sistema informático.
	Interceptación ilícita (Art. 3)	Tipificación de la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.
	Ataques a la integridad de los datos (Art. 4)	Tipificación de todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
	Ataques a la integridad del sistema (Art. 5)	Tipificación de la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
	Abuso de los dispositivos (Art. 6)	Tipificación de la comisión deliberada e ilegítima de actos: a) de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos señalados en las celdas anteriores; ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer los delitos señalados en la celdas anteriores. b) la posesión de algunos de los elementos contemplados en i) o ii) del apartado a) con intención de que sean utilizados para cometer cualquiera de los delitos previstos en las celdas anteriores.
Delitos informáticos	*Falsificación informática* (Art. 7)	Tipificación de la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.
	Fraude informático (Art. 8)	Tipificación de los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Delitos relacionados con el contenido	*Delitos relacionados con la pornografía infantil* (Art. 9)	Tipificación de la comisión deliberada e ilegítima de los siguientes actos: a) producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) oferta o puesta a disposición de pornografía infantil a través de un sistema informático; c) difusión o transmisión de pornografía infantil a través de un sistema informático; d) adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e) posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.[2]
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	*Delitos relacionados con infracciones de la propiedad intelectual y derechos afines* (Art. 10)	Tipificación de las infracciones de la propiedad intelectual que defina su legislación, conforme obligaciones contraídas en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las 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 Derechos de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
		Tipificación de las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artista 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 Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Fuente: BCN, 2011. Revisado, julio 2018

4. Cooperación y asistencia mutua

De acuerdo al Preámbulo del Convenio, ña lucha efectiva contra la Ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penalò

Con este motivo, el texto del acuerdo establece los principios generales relativos a la cooperación internacional (Artículo 23°), a la extradición (Artículo 24°), y a la asistencia mutua (Artículos 25° al 28°). Y en relación a éste última, determina disposiciones específicas en materia de medidas provisionales (como conservación, y revelación rápida de datos informáticos almacenados); de los poderes de investigación (acceso a datos almacenados, acceso y consentimiento transfronterizo, obtención de datos en tiempo real, e interceptación de datos por su contenido); y en particular dispone de la asistencia para establecer una Red 24/7 como punto de contacto localizable las 24 horas del día durante toda la semana que facilite la obtención en formato electrónico de las pruebas de un delito mediante un procedimiento acelerado, garantizando la disponibilidad de personal formado y equipado para estas circunstancias (Artículo 35°).

5. Desarrollo e implementación del Convenio

El Comité del Convenio sobre la Ciberdelincuencia (*Cybercrime Convention Committee*), denominado oficialmente por la sigla T-CY, es el órgano que sirve de consulta entre las Partes, y que tiene por misión facilitar la utilización y aplicación efectiva del tratado, intercambiar información, y estudiar la posibilidad de enmendar o ampliar el acuerdo, según lo establecido en el Artículo 46° de la Convención.

[2] El Convenio entiende por pornografía infantil todo material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. Asimismo, entiende por menor a toda persona menor de 18 años.

Entre las principales funciones que cumple el T-CY se encuentra evaluar la aplicación del Convenio, adoptar opiniones y recomendaciones respecto de su implementación, revisar el funcionamiento del Punto de Contacto 24/7, y promover la adhesión al tratado (Cybercrime Convention Committee, 2016).

Al respecto, el T-CY ha desarrollado un Plan de Acción desde el año 2012, que a la fecha entre sus mayores logros alcanzados ha adoptado ocho Notas Guías (*Guidance Notes*) que representan un común entendimiento entre las Partes referido a la actualización y precisión de la terminología utilizada en el Convenio sobre los siguientes temas: sistema informático (*computer system*), robot informático (*botnets*), ataques de denegación de servicio (*Distributed Denial of Service* DDoS *attacks*), robo de identidad y *phishing*[3] relativo a fraudes (*identity thefts*), ataques a infraestructura de información crítica, nuevas formas de software maligno o *malware*, acceso trasfronterizo a datos (Artículo 32°), y correo basura o *spam* (Cybercrime Convention Committee, 2014).

Actualmente el T-CY desarrolla un Grupo de Trabajo sobre *Cloud Evidence*, cuyo fin es explorar posibles soluciones de acceso para la justicia penal a la evidencia almacenada en servidores en la nube y en jurisdicciones extranjeras (Cybercrime Convention Committee, 2016b).

Asimismo, el Consejo de Europa desarrolla un programa de Ciberdelincuencia denominado *Cybercrime Programme Office* (C-PROC) basado en la Convención con el fin de apoyar y fortalecer la capacidad de la justicia penal de los países para responder a los desafíos del cibercrimen a nivel mundial (COE, 2016b).

Además, el Consejo de Europa realiza en forma periódica, cada 12 a 18 meses una conferencia mundial denominada Octopus que reúne expertos, organismos internacionales, empresarios y académicos frente a un tema específico vinculado al cibercrimen (COE, 2016c).

6. Protocolo Adicional del Convenio

En forma complementaria al tratado, en abril de 2003 se suscribió el Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (*Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*) (STE N°189), que tiene por objeto armonizar la legislación penal sustantiva en relación a la lucha contra el racismo y la xenofobia en Internet, y mejorar la cooperación en esta materia (COE, 2003).

A nivel interno, las Partes contratantes deberán tomar medidas legislativas o de otra índole para evitar la difusión de material racista y xenófobo mediante sistemas informáticos, impedir que mediante las redes se den amenazas o insultos con motivación racista o xenófoba y también impedir que se utilicen sistemas informáticos para negar o justificar genocidios o crímenes contra la humanidad.

II. Legislación contra el Cibercrimen y políticas de Ciberseguridad en Chile

Chile posee normas que resguardan la seguridad del uso de sistemas informáticos, pero algunas se encuentran desactualizadas o el tipo penal está consagrado para otro delito. Por tal motivo, el pasado

[3] De acuerdo a las Guidance Notes, la apropiación indebida de una característica de la identidad personal (nombre, fecha de nacimiento o dirección) sin consentimiento previo, con motivo de obtener bienes o servicios a nombre de esa persona, es un tipo de fraude que se puede realizar mediante actividades de phishing, pharming, spear phising o spoofing, conductas a través de las cuales se intenta acceder a contraseñas u otras credenciales restringidas por medio de correos electrónicos o sitios web falsos.

gobierno evaluó las exigencias de la Convención del Cibercrimen que promueve el Consejo de Europa decidiendo presentarla para su ratificación en el Congreso Nacional (Boletín N° 10.682-10)[4] con el fin de ñperfeccionar el marco jurídico vigente, y así contar con herramientas jurídicas y técnicas modernas para enfrentar de mejor manera la amenaza del cibercrimen, dada su naturaleza transnacional y organizadaò, según el grupo de expertos en incidentes de seguridad de la información, estructura operativa dependiente del Ministerio del Interior y Seguridad Pública *Computer Security Incident Response Team*, CSIRT, Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT, 2016).

El Mensaje Presidencial mediante el que se aprueba el Convenio (Boletín N° 10.682-10) declara en el instrumento de ratificación que aplicará el sentido de su legislación interna a los Artículos 2°, 3° y 7° del tratado, y que se reserva de incorporar a su jurisdicción interna la aplicación de los siguientes aspectos del acuerdo en vigencia:

- tipificar en su derecho interno como delito todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves;
- no aplicar el párrafo 1 del Artículo 6°, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el citado Artículo 6
- no aplicar los apartados b) y c) del párrafo 2 del Artículo 9°
- no aplicar las normas sobre jurisdicción establecidas en el apartado 1 d. del Artículo 22°
- el derecho a denegar la solicitud de asistencia internacional en caso de la que la conducta perseguida no esté tipificada en Chile al momento del requerimiento, conforme a la aplicación del Artículo 29°

1. Marco legal vigente en Chile

En nuestro país el establecimiento en 1993 de la Ley N° 19.223 que tipifica figuras penales relativas a la informática fue pionero en la región latinoamericana (BCN, 2011) al penalizar en sus cuatro artículos las siguientes acciones (Ley N 19.223):

a) la destrucción o inutilización maliciosa de un sistema de tratamiento de información, sus partes o componentes, así como el impedimento, obstaculización o modificación de su funcionamiento;

b) la interceptación, interferencia o acceso a un sistema de tratamiento de la información realizada con el ánimo de apoderarse, usar o conocer indebidamente la información en él contenida;

c) la alteración, daño o destrucción de los datos contenidos en un sistema de tratamiento de información; y

d) la revelación o difusión maliciosa de los datos contenidos en un sistema de información.

Sin embargo, el desarrollo actual de la tecnología ha dejado en evidencia el retraso de la norma que no incorpora algunas figuras delictivas de importancia, como son el fraude informático o el *hacking* directo (acceso no autorizado), así como su insuficiencia para enfrentar las nuevas formas delictivas que surgen en relación al mal uso de las tecnologías de la información, como por ejemplo la creación y distribución de virus y programas dañinos (figura que para algunos autores no debiera quedar cubierta por el sabotaje informático) o la falsificación de documento electrónico, entre otras (BCN, 2011).

[4] El Convenio sobre Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001, fue aprobado por el Congreso Nacional de Chile el 16 de mayo de 2016, promulgado por el D.S. N° 83, y publicado en el Diario Oficial el 28-8-2017.

Existen también otros instrumentos legales que brindan seguridad al uso de sistemas informáticos, según el CSIRT del Ministerio del Interior y Seguridad Pública el marco legal vigente está compuesto además por:

- Ley N°20.285 sobre acceso a la información pública
- Ley N°19.927 modifica códigos penales en materia de delitos sobre pornografía infantil
- Ley N°19.880 establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado
- Ley N°19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
- Ley N°19.628 sobre protección de la vida privada , y
- Ley N°17.336 sobre propiedad intelectual.

III. Anexos

Anexo N°1: Países de Europa que han Ratificado el Convenio de Budapest

País	Firma	Ratificación
ALBANIA	23-11-2001	20-06-2002
ALEMANIA	23-11-2001	09-03-2009
ANDORRA	23-04-2013	16-11-2016
ANTIGUA REPUBLICA YUGOSLAVA DE MACEDONIA	23-11-2001	15-09-2004
ARMENIA	23-11-2001	12-10-2006
AUSTRIA	23-11-2001	13-06-2012
AZERBAIJAN	30-6-2008	15-03-2010
BELGICA	23-11-2001	20-08-2012
BOSNIA Y HERZEGOVINA	09-02-2005	19-05-2006
BULGARIA	23-11-2001	07-04-2005
CHIPRE	23-11-2001	19-01-2005
CROACIA	23-11-2001	17-10-2002

DINAMARCA	22-04-2003	21-06-2005
ESLOVENIA	24-07-2002	08-09-2004
ESPAÑA	23-11-2001	03-06-2010
ESTONIA	23-11-2001	12-05-2003
FINLANDIA	23-11-2001	24-05-2007
FRANCIA	23-11-2001	10-01-2006
GEORGIA	01-04-2008	06-06-2012
GRECIA	23-11-2001	25-01-2017
HUNGRIA	23-11-2001	04-12-2003
ISLANDIA	30-11-2001	29-01-2007
ITALIA	23-11-2001	05-06-2008
LETONIA	05-05-2004	14-02-2007
LIECHTENSTEIN	17-11-2008	27-01-2016
LITUANIA	23-06-2003	18-03-2004
LUXEMBURGO	28-01-2003	16-10-2014
MALTA	17-01-2002	12-04-2012
MONACO	02-05-2013	17-03-2017
MONTENEGRO	07-04-2005	03-03-2010
NORUEGA	23-11-2001	30-06-2006
PAISES BAJOS	23-11-2001	16-11-2006
POLONIA	23-11-2001	20-02-2015
PORTUGAL	23-11-2001	24-03-2010
REINO UNIDO	23-11-2001	25-05-2011
REPUBLICA CHECA	09-02-2005	22-08-2013
REPUBLICA DE MOLDAVA	23-11-2001	12-05-2009
REPUBLICA ESLOVACA	04-02-2005	08-01-2008
RUMANIA	23-11-2001	12-05-2004
SERBIA	07-04-2005	14-04-2009

SUIZA	23-11-2001	21-09-2011
TURQUIA	10-11-2010	29-09-2014
UCRANIA	23-11-2001	10-03-2006

Fuente: Elaboración propia con información disponible en https://rm.coe.int (Julio, 2018)

Anexo N°2: Países europeos que han Firmado pero no Ratificado Budapest

País	Firma
IRLANDA	30-11-2001
SAN MARINO	17-03-2017
SUECIA	23-11-2001

Fuente: Elaboración propia con información disponible en https://rm.coe.int (Julio, 2018)

Anexo N°3: Países no miembros del Consejo de Europa que han Ratificado Budapest

País	Firma	Ratificación
ARGENTINA		05-06-2018
AUSTRALIA		30-11-2012
CABO VERDE		19-06-2018
CANADA	23-11-2001	08-07-2015
CHILE	23-11-2001	20-04-2017
COLOMBIA		20-06-2018
COSTA RICA		22-09-2017
ESTADOS UNIDOS	23-11-2001	29-09-2006
FILIPINAS		28-03-2018
ISRAEL		09-05-2016
JAPON	23-11-2001	03-07-2012
MAURICIO		15-11-2013
MARRUECOS		29-06-2018

PANAMA		05-03-2014
REPUBLICA DOMINICANA		07-02-2013
SENEGAL		16-12-2016
SRI LANKA		29-05-2015
TONGA		09-05-2017

Fuente: Elaboración propia con información disponible en https://rm.coe.int (Julio, 2018)

Anexo N°4: Países invitados a integrarse al Convenio de Budapest

País
GHANA
NIGERIA
PARAGUAY
PERU
TONGA
TUNEZ

Fuente: Elaboración propia con información disponible en https://rm.coe.int (Julio, 2018)

Referencias

BCN (2011) ñDelitos a través de la red. El Convenio de Budapest como un ejemplo de armonización legislativa y el ordenamiento jurídico chileno ante el ciberdelitoò Informe BCN elaborado por Blanca Bórquez, 21-11-2011. Disponible en: http://repositorio.bcn.cl Julio, 2018)

BCN (2016) ñConvenio de Budapest sobre la Ciberdelincuencia y situación de la Ciberseguridad en Chileò Informe BCN elaborado por Andrea Vargas, 21-11-2011. Disponible en: http://repositorio.bcn.cl Julio, 2018)

CÁMARA DE DIPUTADOS (2010)Proyecto de Acuerdo N° 231, solicitando al Presidente de la República, la Adhesión del Estado de Chile al Convenio Internacional sobre Ciberdelincuencia, Sesión 101 de la Cámara de Diputados, celebrada el 16-11-2010. Disponible en: https://www.camara.cl/prensa/noticias_detalle.aspx?prmid=42517 (Julio, 2018)

CÁMARA DE DIPUTADOS (2016) Proyecto de Acuerdo que Aprueba el Convenio Sobre la Ciber-Delincuencia. Boletín N° 10.682-10. Disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11105&prmBoletin=10682-10 (Julio, 2018)

COE (2001) Informe Explicativo Convenio sobre la Ciberdelincuencia. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403 (Julio, 2018)

Decreto N° 533, 17-07-2015. Crea Comité Interministerial sobre Ciberseguridad. Disponible en: http://bcn.cl/1rra5 (Julio, 2018)

Ministerio de Relaciones Exteriores de Chile. ñChile deposita el instrumento de adhesión al Convenio de Budapest sobre la Ciberdelincuenciaò Disponible en: https://minrel.gob.cl (Julio, 2018)

Ley N° 19.223 de 07-06-1993. Tipifica figuras penales relativas a la informática. Disponible en: http://bcn.cl/1uw5c (Julio, 2018)