BCN Informe

Biblioteca del Congreso Nacional de Chile

Convenio sobre la Ciberdelincuencia y situación de la Ciber Seguridad en Chile

En la sociedad actual, el acceso universal a Internet y el desarrollo de las nuevas tecnologías han influido en que la conexión a la red esté presente en la evidencia electrónica de casi cualquier tipo de delito, situación que requiere de un cambio de enfoque en la aproximación legal interna e internacional frente al fenómeno transnacional de la ciberdelincuencia.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) es el acuerdo internacional más utilizado para desarrollar la legislación de combate al cibercrimen, no obstante, existen otros acuerdos multilaterales que regulan la materia en distintas regiones del mundo. El Convenio de Budapest ha sido ratificado por 47 Estados, incluidos los 28 Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia, Japón, Sudáfrica y República Dominicana. Por su parte, Chile ha sido invitado a adherirse a él, no obstante el gobierno está evaluando las implicancias jurídicas de ratificar el Convenio.

En síntesis, la Convención 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 se encuentra la obligación de las Partes de tipificar delitos contra la integridad de los sistemas o datos informáticos y respecto de su contenido, así como establecer procedimientos que faciliten la investigación penal, principalmente a través de exigir la conservación, registro, interceptación y confiscación de los datos almacenados. 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 de seguridad 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 en términos de los organismos responsables de la protección, ésta se encuentra compartida en diferentes organismos estatales.

Por estos motivos, el gobierno determinó durante este año crear el Comité Interministerial sobre Ciberseguridad, organismo asesor presidencial de carácter permanente, con el fin de elaborar una Política Nacional de Ciberseguridad que podría ser publicada en marzo de 2016.

Biblioteca del Congreso Nacional de Chile. Asesoría Técnica Parlamentaria. Área de Gobierno, Defensa y Relaciones Internacionales. Andrea Vargas Cárdenas – avargas@bcn.cl – Anexo 1871. 29/12/2015.

Tabla de Contenido

I. Introducción

Este informe aborda en forma descriptiva las implicancias que el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) –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.

Asimismo, se presentan las medidas adoptadas en Chile en materia de ciberseguridad, indicando el marco legal vigente aplicable a los ciberdelitos; el establecimiento de una estrategia de seguridad digital enfocada en la creación de un Comité Interministerial sobre Ciberseguridad; el desarrollo de una Política Nacional en la materia, así como la participación más activa de nuestro país en foros de alcance global sobre seguridad digital.

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 "*Comprehensive Study on Cibercrime*", 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[1].

---

[1] UNODC: *Comprehensive Study on Cibercrime.* Feb-2013. Disponible en: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Diciembre, 2015).

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[2].

Al respecto, el estudio señala que a nivel mundial son 82 Estados los que han ratificado algún instrumento internacional de lucha contra el cibercirmen[3], 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[4].

II. Convenio del Consejo de Europa sobre Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia (*Convention on Cybercrime*), conocido como Convenio de Budapest (Serie Tratados Europeos N° 185)[5], fue suscrito en dicha ciudad el 23 de noviembre de 2001 en el marco de los Estados miembros del Consejo de Europa[6], y se encuentra en vigor a partir del 1 de julio de 2004.

1. Objetivo

El Convenio de Budapest, según establece su Preámbulo tiene por fin "incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos"[7], mediante "una cooperación internacional reforzada, rápida y eficaz en materia penal"[8].

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

---

[2] Ibíd. Pág. xi

[3] 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).*

[4] UNODC: Op. Cit. Pág. XIX.

[5] Consejo de Europa: Convenio sobre la Ciberdelincuencia. STE N° 185, Budapest, 23-11-2001. Disponible en: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_spanish.PDF (Diciembre, 2015).

[6] El Consejo de Europa (COE, por su sigla en inglés), es una organización de carácter regional que reúne a 47 Estados del continente europeo con el objetivo de promover la defensa y protección de la democracia, el Estado de Derecho y los derechos humanos.

[7] Consejo de Europa: Convenio sobre la Ciberdelincuencia. STE N° 185. Preámbulo. *Op. Cit.*

[8] *Ibíd.*

del Convenio[9], 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[10].

No obstante, una de las principales críticas al Convenio de Budapest ha sido que sus disposiciones procedimentales no se limitan solo al ciberdelito, sino más bien a cualquier tipo de delito para el cual sea necesario reunir evidencia en formato electrónico. Al respecto, Michael Vatis, abogado experto en derecho y seguridad informática, ha señalado que en estos asuntos la Convención obliga a los Estados Parte a establecer leyes que faculten el registro y confiscación de computadores y datos informáticos almacenados en ellos, así como la interceptación de datos e intervención de redes para obtener información en tiempo real, más allá de si el delito bajo investigación es o no un ciberdelito propiamente tal[11].

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[12]. De este modo, en la región latinoamericana han sido invitados a adherirse al Convenio Argentina, Chile, Colombia, Costa Rica, México y Panamá, y Paraguay y Perú han manifestado interés en incorporarse a éste[13]. A la fecha, Budapest ha sido ratificado por 47 Estados[14], actualmente son Parte del tratado los 28 Estados miembros de la Unión Europea, y otros ocho países no europeos[15], entre ellos Estados Unidos, Canadá, Australia, Japón, Sudáfrica y República Dominicana. 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).

---

[9] El Informe Explicativo de 2001, según se establece textualmente, no constituye una interpretación autorizada. Ver COE: Convenio sobre la Ciberdelincuencia. Informe explicativo. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403 (Diciembre, 2015).

[10] COE: Convenio sobre la Ciberdelincuencia. Informe explicativo. Párr. 16. *Op. Cit.* Ver también VATIS, Michel: The Council of Europe Convention on Cybercrime. Disponible en: http://www.nap.edu/catalog/12997.html (Diciembre, 2015).

[11] VATIS, Michael: *Op. Cit.* pág. 208.

[12] Consejo de Europa: Convenio sobre la Ciberdelincuencia. STE N° 185. *Op. Cit.*

[13] COE: Memoria del "Taller sobre Legislación en materia de Ciberdelincuencia en América Latina". 31 de marzo al 2 de abril de 2014. Pág. 135. Disponible en: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/2014/Memoria%20Taller%20Ciberdelito.pdf (Diciembre, 2015).

[14] COE: *Chart of signatures and ratifications of Treaty* 185. Actualizado al 18 de diciembre de 2015. Disponible en: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=5TIA6YU0 (Diciembre, 2015).

[15] Durante el periodo de negociaciones Canadá, Japón, Sudáfrica y Estados Unidos participaron de la preparación del tratado en calidad de Observadores.

3. Medidas que los Estados Parte deben adoptar

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[16].

a. Contenido de derecho penal sustantivo

La siguiente tabla sintetiza la tipificación de los delitos de acuerdo al texto del tratado[17].

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.

[16] BÓRQUEZ, Blanca: "Delitos a través de la red. El Convenio de Budapest como un ejemplo de armonización legislativa y el ordenamiento jurídico chileno ante el ciberdelito". BCN Informe, 21-11-2011. Disponible en: http://repositorio.bcn.cl (Diciembre, 2015).
[17] *Ibíd.*

		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.[18]
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: BÓRQUEZ, Blanca: "Delitos a través de la red. El Convenio de Budapest como un ejemplo de armonización legislativa y el ordenamiento jurídico chileno ante el ciberdelito". BCN Informe, 21-11-2011. Disponible en: http://repositorio.bcn.cl (Diciembre, 2015).

Además, también deberán ser sancionadas las figuras de tentativa y complicidad en los delitos tipificados[19], y exigir responsabilidad penal a las personas jurídicas[20].

---

[18] 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.

[19] Artículo 11º.

[20] Artículo 12º.

Asimismo, el Convenio dispone que las sanciones deberán ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad[21] [22].

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°); y la interceptación de datos relativos al contenido de las comunicaciones (Artículo 21°).

4. Cooperación y asistencia mutua

De acuerdo al Preámbulo del Convenio, "la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal"[23].

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°).

---

[21] Artículo 13º. Sanciones y medidas.
[22] FINSTERBUSCH, Christian: "Convenio de Budapest sobre Ciber-delincuencia y efectos derivados de la posible adhesión por parte de Chile". BCN Informe, 04-10-2011. Disponible en: http://repositorio.bcn.cl (Diciembre, 2015).
[23] Consejo de Europa: Convenio sobre la Ciberdelincuencia. STE N° 185. *Op. Cit.*

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.

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[24]. 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*[25] 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*[26].

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[27].

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[28].

Además, el Consejo de Europa realiza en forma periódica, cada 12 a 18 meses una conferencia mundial denominada Octopus que reúne expertos, organismos

---

[24] *Cybercrime Convention Committee*: T-CY *Workplan for the period 1 January 2016 – 31 December 2017*. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804924d2 (Diciembre, 2015).

[25] 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.

[26] *Cybercrime Convention Committee: T-CY Guidances Notes.* 8-12-2014. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804668b06 (Diciembre, 2015).

[27] *Cybercrime Convention Committee: Cloud Evidence Group.* Disponible en: http://www.coe.int/en/web/cybercrime/ceg (Diciembre, 2015).

[28] COE: *Worldwide Capacity Building*. Disponible en: http://www.coe.int/en/web/cybercrime/capacity-building-programmes (Diciembre, 2015).

internacionales, empresarios y académicos frente a un tema especifico vinculado al cibercrimen[29].

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[30].

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[31].

A la fecha, el protocolo Adicional ha sido ratificado por 24 Estados, y aunque está abierto a la suscripción de Estados no europeos, hasta ahora todos los países que lo han ratificado son miembros del Consejo de Europa[32].

III. 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 gobierno actual se encuentra en "proceso de evaluación de la Convención del Cibercrimen que promueve el Consejo de Europa"[33], con el fin de "perfeccionar el marco jurídico vigente, y así contar con herramientas jurídicas y técnicas modernas para enfrentar de mejor manera la

---

[29] COE: *Octopus Conferences*. Disponible en: http://www.coe.int/en/web/cybercrime/octopus-conference (Diciembre, 2015).
[30] COE: *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. 28-01-2003. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d37ae (Diciembre, 2015).
[31] BARRIOS, Verónica: Convenio N° 185 del Consejo de Europa sobre la Ciberdelincuencia o Convenio de Budapest. BCN Minuta. Disponible en: http://repositorio.bcn.cl (Diciembre, 2015).
[32] COE: Chart of signatures and ratifications of Treaty 189. Disponible en: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=ruIfdXNG (Diciembre, 2015).
[33] CSIRT - Ministerio del Interior y Seguridad Pública: Convención del Cibercrimen. Disponible en: http://www.csirt.gob.cl/convencion_cibercrimen.html (Diciembre, 2015).

amenaza del cibercrimen, dada su naturaleza transnacional y organizada"[34], de acuerdo al grupo de expertos en incidentes de seguridad de la información, estructura operativa dependiente del Ministerio del Interior y Seguridad Pública (CSIRT, *Computer Security Incident Response Team*, Equipo de Respuesta a Incidentes de Seguridad Cibernética).

7. 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[35] al penalizar en sus cuatro artículos las siguientes acciones[36]:

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[37].

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[38]:

- Ley N°20.285 sobre acceso a la información pública[39]
- Ley N°19.927 modifica códigos penales en materia de delitos sobre pornografía infantil[40]

---

[34] *Ibíd.*
[35] BÓRQUEZ, Blanca: *Op. Cit.*
[36] Ley N° 19.223 Tipifica figuras penales relativas a la informática Disponible en: http://bcn.cl/1m196 (Diciembre, 2015).
37 BÓRQUEZ, Blanca: *Op. Cit.*
38 CSIRT - Ministerio del Interior y Seguridad Pública: Leyes. Disponible en: http://www.csirt.gob.cl/leyes.html (Diciembre, 2015).
39 http://bcn.cl/1lze1 (Diciembre, 2015).
40 http://bcn.cl/1mh5w (Diciembre, 2015).

- Ley N°19.880 establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado[41]
- Ley N°19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma[42]
- Ley N°19.628 sobre protección de la vida privada[43], y
- Ley N°17.336 sobre propiedad intelectual[44].

8. Estrategia de seguridad digital en Chile

Según un informe del año 2013 elaborado por la Organización de los Estados Americanos (OEA), en nuestro país no existe información cuantitativa suficiente para evaluar el tema de las ciber amenazas, sin embargo, los mayores incidentes de seguridad en Chile se relacionan con actividades de *phishing*, *malware* o programas maliciosos y el *hackeo* de páginas Web gubernamentales por parte de *hacktivistas,* así como también han aumentado las denuncias de *grooming* (captación de menores con fines sexuales) y las amenazas contra personas[45].

La responsabilidad en la promoción de la seguridad cibernética y en la lucha contra la ciberdelincuencia se encuentra compartida en varios organismos estatales: el Ministerio del Interior y Seguridad Pública, la Secretaría General de la Presidencia y la Subsecretaría de Telecomunicaciones; y por otra parte, la investigación criminal la desarrollan tanto la Brigada Investigadora del Ciber Crimen (BRICIB) de la Policía de Investigaciones, como el Departamento de Investigación de Organizaciones Criminales (OS-9) y el Departamento de Criminología, ambos de Carabineros de Chile[46].

Para una mejor coordinación entre las acciones, planes y programas de estos distintos actores y con el fin de elaborar una Política Nacional de Ciberseguridad, el gobierno determinó en abril de 2015 la creación del Comité Interministerial sobre Ciberseguridad (CIC), organismo de carácter permanente, que asesora al Presidente de la República, y que está integrado por ocho miembros, cada uno en representación de: la Subsecretaría del Interior, Subsecretaría de Defensa, Subsecretaría de Relaciones Exteriores, Subsecretaría de Justicia, Subsecretaría General de la Presidencia, Subsecretaría de Telecomunicaciones, Subsecretaría de Economía y Empresas de Menor Tamaño y la Dirección Nacional de la Agencia Nacional de Inteligencia[47].

---

41 http://bcn.cl/1m07f (Diciembre, 2015).
42 http://bcn.cl/1lzdc (Diciembre, 2015).
43 http://bcn.cl/1lyp5 (Diciembre, 2015).
44 http://bcn.cl/1m035 (Diciembre, 2015).
45 OEA – Symantec: Tendencias de seguridad cibenética en América Latina y el Caribe. Junio, 2014. Disponible en: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf (Diciembre, 2015).
46 *Ibíd.*
47 Decreto N° 533, 17-07-2015. Crea Comité Interministerial sobre Ciberseguridad. Disponible en: http://bcn.cl/1rra5 (Diciembre, 2015).

Para efectos de desarrollar su cometido, en el decreto de creación del Comité el gobierno definió que la ciberseguridad es: "aquella condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones que se verifican en el ciberespacio, como también el conjunto de políticas y técnicas destinadas a lograr dicha condición"[48].

De acuerdo a lo que ha sido difundido en los medios de comunicación, se espera que la Política Nacional de Ciberseguridad esté finalizada en marzo de 2016[49], y que tenga por objetivo "promover la identificación y gestión de riesgos en el ciberespacio para que el sector público, privado, la sociedad civil y el mundo académico puedan prevenir, minimizar y sobreponerse a éstos, con especial énfasis en aquellas infraestructuras críticas para el funcionamiento del país, tales como los servicios de telecomunicaciones, de electricidad o de agua potable, el transporte público o los servicios financieros, junto con las instituciones que resguardan la seguridad y soberanía de nuestro país, como la Defensa Nacional"[50].

Además, el gobierno decidió asistir y participar por primera vez en la Conferencia Global del Ciberespacio, realizada en La Haya, en abril de 2015, a través de los Subsecretarios de Relaciones Exteriores, Edgardo Riveros, y de Telecomunicaciones, Pedro Huichalaf, junto a representantes de otros ministerios, con el objetivo de "adoptar un papel activo en las instituciones y procesos que conforman la gobernanza de internet; [y] promover el valor del ciberespacio como un bien público global, donde se avance hacia nuevas formas de gobernanza de bienes comunes y que involucre a múltiples partes involucradas" [51].

Por otra parte, y más allá que el Gobierno afirme estar evaluando las exigencias del Convenio de Budapest sobre Ciberdelincuencia, en el Congreso Nacional han sido aprobados con fechas distintas en la Cámara de Diputados y en el Senado sendos Proyectos de Acuerdo solicitando al Ejecutivo la adhesión del Estado de Chile al Convenio sobre Ciberdelincuencia del Consejo de Europa[52].

---

[48] Ibíd. Artículo 7°.

[49] Cooperativa.cl: Gobierno anunciará su política nacional de ciberseguridad en marzo próximo. 27/11/2015. Disponible en: http://www.cooperativa.cl/noticias/tecnologia/industria/gobierno-anunciara-su-politica-nacional-de-ciberseguridad-en-marzo/2015-11-27/170450.html (Diciembre, 2015).

[50] ROBLEDO, Marcos: Discurso seminario ciberseguridad - Marcos Robledo Hoecker, Subsecretario de Defensa. Facultad de Derecho de la Universidad de Chile. 27/11/2015. Disponible en: http://163.247.42.118/Documentospla/discursossdseminariociberuchile27nov.pdf (Diciembre, 2015).

[51] Ministerio de Relaciones Exteriores de Chile: Subsecretario Riveros viaja a La Haya para participar en Conferencia Global del Ciberespacio. 14-04-2015. Disponible en: http://www.minrel.gob.cl/subsecretario-riveros-viaja-a-la-haya-para-participar-en-conferencia-global-del-ciberespacio/minrel/2015-04-14/150737.html (Diciembre, 2015).

[52] 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 (Diciembre, 2015); Proyecto de Acuerdo presentado en la sesión 137, de 10 de marzo de 2011 con el objeto de solicitar la adhesión del Estado de Chile al Convenio de Budapest. Disponible en: http://www.camara.cl/pdf.aspx?prmid=8799&prmtipo=TEXTOSESION (Diciembre, 2015); y Proyecto de Acuerdo del Senado por el que Solicitan a S. E. la Presidenta de la República encomiende al señor Ministro de Relaciones Exteriores realizar gestiones para la adhesión de Chile al Convenio sobre

Ciberdelincuencia o Convención de Budapest, y que, asimismo, instruya al señor Ministro del Interior y Seguridad Pública para que evalúe la reactivación de la "Comisión de Trabajo Interministerial Conducente a la Adhesión de Chile a la Convención sobre Ciber Delitos del Consejo de Europa", creada por decreto supremo N ° 326, de Interior, de 2009. Boletín N° 1737-12 30/12/2014. Disponible en: http://www.senado.cl/appsenado/index.php?mo=consultas as oa&ac=Get documentoAS&iddocto=1976 &tipodoc=35 (Diciembre, 2015).