Universidad de Chile

Facultad de Derecho

Departamento de Derecho Internacional

LA RECEPCIÓN E INCORPORACIÓN DEL PRINCIPIO DE COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERSEGURIDAD EN EL DERECHO CHILENO

Memoria de prueba para optar al grado de Licenciado en Ciencias Jurídicas y Sociales

Profesor Guía: CLAUDIO TRONCOSO REPETTO

MARÍA CONSUELO GÁLVEZ REYES

RAIMUNDO GÁLVEZ PACHECO

Santiago, Chile

2020

AGRADECIMIENTOS

Queremos agradecer a nuestras familias y amigos, por acompañarnos y apoyarnos durante estos 5 años de carrera. También queremos extender nuestros agradecimientos en forma especial al profesor Claudio Troncoso, por guiar este trabajo y entregarnos las herramientas necesarias para su elaboración.

ÍNDICE

RESUMEN

El objetivo del presente trabajo es dilucidar si en Chile se ha incorporado efectivamente el principio de cooperación internacional al legislar sobre materias de ciberseguridad, especialmente considerando su importancia como uno de los principios rectores que contempla el Convenio sobre la Ciberdelincuencia ratificado por Chile y promulgado en agosto de 2017 mediante el D.S 83/2017.

Esta memoria comienza con un estudio de la normativa vigente en materia de ciberseguridad tanto a nivel nacional como internacional, que analiza cómo cada una de estas ha recepcionado el principio de cooperación internacional.

A partir de lo anterior, este trabajo busca determinar si el Estado chileno, en su legislación vigente, ha logrado establecer un marco normativo e institucional que dé cumplimiento a su obligación internacional de cooperar jurídicamente en materia de ciberseguridad, conforme a lo dispuesto en el Convenio de Budapest.

La memoria culmina con un análisis de las consecuencias para Chile de no contar, en el largo plazo, con un marco normativo e institucional ajustado al principio de cooperación internacional en esta materia, junto con la presentación de las conclusiones.

INTRODUCCIÓN

En la actualidad, vivimos en una época en la que el desarrollo de la tecnología se produce de manera exponencial y a una velocidad que es prácticamente imposible de seguir. Se trata de un periodo de la historia marcado por procesos de globalización que difuminan cada vez más las fronteras tradicionales entre los Estados y, en consecuencia, hacen cada vez más necesaria su integración, coordinación y cooperación en torno a diversas materias.[1] Vivimos en un mundo que hoy gira de manera casi absoluta en torno a Internet y que se rige en base a las relaciones que se producen en el ciberespacio. Considerando todos estos fenómenos sociales —y que el derecho no es más que un instrumento flexible que evoluciona de la mano del "organismo vivo",[2] que es la sociedad que busca regular—, cabe plantearse la siguiente pregunta: ¿cómo se ha adecuado el derecho a estos importantes avances tecnológicos?, y más específicamente, ¿cómo se ha adaptado el derecho *chileno* a todas estas transformaciones?

Producto de las innovaciones tecnológicas y sociales marcadamente globalizadas que se han presentado en las últimas décadas, una de las mayores dificultades que ha surgido para los ordenamientos jurídicos del mundo ha sido el enfrentarse al mundo digital. Dentro de este contexto, hemos sido testigos del desarrollo —cada vez más complejizado— de una nueva categoría de delitos: la ciberdelincuencia. Es así como el surgimiento del ciberespacio como dominio virtual de interacciones sociales ha dado lugar también a nuevas amenazas para la seguridad, las cuales requieren ser combatidas por los Estados.[3] Dada su naturaleza digital, estos nuevos delitos trascienden toda noción clásica de fronteras entre países, razón por la cual exigen de forma urgente que exista una fuerte cooperación internacional para su regulación y persecución.[4] Debido a esto, resulta necesario analizar cómo (y si es que) el marco normativo chileno ha respondido adecuadamente a este fenómeno, particularmente a

[1] Rafael Domingo, "¿Por qué un Derecho Global?", en *Hacia un Derecho Global: Reflexiones en torno al Derecho y la Globalización*, coord. Aparicio Caicedo, Rafael Domingo y Martín Santiváñez (Cizur Menor, Navarra: Editorial Aranzadi, 2006), 21–24.
[2] Jean Carbonnier, *Derecho flexible. Para una sociología no rigurosa del Derecho* (Madrid: Ed. Tecnos, 1974), 16–21.
[3] Carolina Sancho Hirane, "Ciberinteligencia: Contextualización, Aproximación Conceptual, Características y Desafíos", *Cuaderno de trabajo* 1 (Santiago: Centro de Investigaciones y Estudios Estratégicos, marzo 2018), en línea, consulta: 29 de agosto de 2019, disponible: https://www.anepe.cl/wp-content/uploads/Cuaderno-Trabajo-N%C2%B01-2018.pdf.
[4] Ana I. Cerezo, Javier Lopez y Ahmed Patel, "International Cooperation to Fight Transnational Cybercrime", *Second international workshop on digital forensics and incident analysis* (WDFIA, 2007), 14.

la luz del principio de cooperación internacional plasmado en la normativa internacional vigente.

Dentro de este contexto, la presente memoria buscará responder la siguiente pregunta: **¿Se ha incorporado exitosamente en el derecho chileno el principio de cooperación internacional al regular materias de ciberseguridad?**

Nuestra investigación tiene como objeto primordial analizar el marco normativo e institucional vigente en Chile y determinar si en él se ha incorporado efectivamente el principio de cooperación internacional al regular materias de ciberseguridad, especialmente considerando su importancia como uno de los principios fundantes del *Convenio sobre la Ciberdelincuencia* o Convenio de Budapest del año 2001, ratificado por Chile y promulgado en agosto de 2017 mediante el DS 83/2017.[5] Para responder la pregunta de investigación señalada, el presente trabajo se estructura en base a cuatro capítulos: **(I)** marco conceptual, **(II)** normativa internacional en materia de ciberseguridad, **(III)** normativa chilena en materia de ciberseguridad y **(IV)** análisis del cumplimiento del Estado chileno de sus obligaciones internacionales en materia de ciberseguridad.

En el primer capítulo del trabajo se abordarán, a modo introductorio, los conceptos generales relacionados a la ciberseguridad, junto con las características que hacen especialmente necesario regular estos delitos de acuerdo con el principio de cooperación internacional, abordando la importancia de este último como un principio imperante en el derecho internacional.

En el segundo capítulo, se estudiará la normativa internacional vigente en materia de ciberseguridad, sus antecedentes históricos, los instrumentos en los cuales ha sido recogida y el énfasis que se le ha dado al principio de cooperación internacional entre Estados a este respecto.

En el tercer capítulo, se realizará un panorama histórico de la legislación nacional en materia de ciberseguridad, para luego examinar críticamente nuestra regulación jurídica actual en

[5] Chile, Ministerio de Relaciones Exteriores, Decreto 83, Promulga el Convenio Sobre la Ciberdelincuencia (28 de agosto de 2017), en línea, consulta: 27 de agosto de 2019, disponible: https://www.leychile.cl/Navegar?idNorma=1106936.

esta materia. Con ello, buscaremos determinar si el principio de cooperación internacional ha sido debidamente recogido en las distintas leyes que han regulado el tema en nuestro derecho interno y si está siendo considerado en las discusiones parlamentarias actuales al respecto.

En el cuarto capítulo, se analizará el cumplimiento por parte del Estado chileno de su obligación de contar con un marco normativo e institucional en materia de ciberseguridad ajustado a los actuales estándares de cooperación internacional, y la eventual responsabilidad en la que podría incurrir Chile – a largo plazo – en caso de que su marco normativo interno no se ajuste a los estándares internacionales exigibles.

Finalmente, el trabajo culminará con una conclusión que, a partir de los hallazgos de la investigación, procurará responder la pregunta inicialmente presentada.

CAPÍTULO I: MARCO CONCEPTUAL

1. Conceptos relacionados con la ciberseguridad

A medida que la tecnología de la información se integra cada vez más en nuestra vida cotidiana, nos vamos transformando rápidamente en una sociedad cibernética. En el mundo actual, una amplia gama de áreas críticas de nuestro desarrollo, desde el suministro de agua hasta el transporte, desde la energía hasta las tecnologías de comunicación, son vulnerables a los ciberataques. Sin embargo, pese a su enorme importancia, estas infraestructuras tienen ninguna o escasa protección cibernética y se basan en soluciones de seguridad que se encuentran completamente obsoletas.[6]

Es así como los últimos adelantos digitales que han irrumpido en décadas recientes a nivel global han generado la aparición de una terminología completamente nueva, la cual resulta desconocida para la mayoría de las personas. Por ello, es de la mayor importancia para el desarrollo de este trabajo determinar las diferencias entre los distintos conceptos que han surgido a propósito de la ciberseguridad, con el fin de lograr una comprensión acabada de las diferentes cuestiones que aquí se plantearán. Los términos a los cuales haremos referencia no pretenden explicar todas las aristas de esta disciplina, sino solo sentar una base teórica mínima con fines didácticos. Estos son: (i) ciberespacio, (ii) ciberseguridad y, finalmente, (iii) ciberdelito.

1.1 Ciberespacio

Actualmente, el ciberespacio es la última dimensión o dominio reconocido en el cual las personas, organizaciones e instituciones a nivel nacional, internacional y transnacional interactúan con la finalidad de comunicarse, intercambiar bienes o servicios, generar valor agregado a productos, entre otros.[7] Tratándose de un área del conocimiento relativamente nueva y de un alto carácter técnico, no resulta extraño que existan diversas nociones a nivel

[6] Murat Dogrul, Adil Aslan y Eyyup Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", *3rd International Conference on Cyber Conflict* (Tallinn, 2011), 30.
[7] Sancho Hirane, "Ciberinteligencia: Contextualización, Aproximación Conceptual, Características y Desafíos", 2.

académico y legal de lo que se entiende por ciberespacio, las cuales otorgan preponderancia a diferentes elementos de este.

A nuestro juicio, la definición propuesta por los profesionales del Cooperative Cyber Defense Centre of Excellence de la OTAN, Rain Ottis y Peeter Lorents, recoge de manera omnicomprensiva los diferentes fenómenos que forman parte de lo que conocemos como ciberespacio. Según ellos, este concepto se entiende como un "*conjunto de sistemas de información interconectados, dependientes del tiempo, y los usuarios humanos que interactúan con dichos sistemas"*.[8] A continuación, nos referiremos a cada uno de los elementos de la definición propuesta:

a. Sistemas de información interconectados: Este punto hace alusión a toda la información, hardware, software y los medios que los conectan.[9] En el caso del hardware, según la Real Academia Española, este se compone de todos los elementos físicos o materiales que constituyen una computadora o un sistema informático. Encontramos dentro de esta categoría el monitor, el CPU, la placa madre, entre otros. Por su parte, cuando hablamos de software, también según la Real Academia Española, nos referimos al conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. Aquí encontramos los diferentes sistemas operativos que usamos a diario, tales como Windows, Linux y Mac.

b. Dependientes del tiempo: Este elemento alude a que los usuarios y las conexiones que componen los sistemas interconectados descritos en el punto anterior pueden aparecer y desaparecer, pues la información se transforma con el tiempo.[10] En otras palabras, la red no es estática, pudiendo producirse cambios dramáticos en tan solo instantes.

c. Usuarios humanos: Esta última característica se refiere a que el ciberespacio es completamente artificial, por lo que, sin usuarios humanos, este se estancaría, se deterioraría y eventualmente dejaría de existir. A menos que algo más pueda hacerse

[8] Peter Lorents, Rain Ottis y Raul Rikk, "Cyber Society and Cooperative Cyber Defence", *International Conference on Internationalization, Design and Global Development* (Springer, Berlín y Heidelberg, 2009), 2.
[9] Ibid., 2-3.
[10] Ibid.

> cargo del mantenimiento y el desarrollo de la infraestructura y el contenido cibernéticos. En consecuencia, el ser humano sigue siendo una parte importante del ciberespacio.[11]

En el caso chileno, dos documentos oficiales abordan conceptualmente este término en forma similar. En efecto, el texto "Bases para una Política Nacional de Ciberseguridad", publicado en 2015, define el concepto de ciberespacio como "un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior", mientras que en la Política Nacional de Ciberseguridad (PNCS), publicada en 2017, la misma expresión es entendida como "el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren", constatándose una aproximación coincidente en todas ellas.[12]

1.2 Ciberseguridad

Al igual que en el caso del ciberespacio, nos encontramos con que no existe una noción universalmente aceptada que precise qué se entiende por ciberseguridad. No obstante, una definición que expone de forma muy clara las distintas características de este concepto es la que entrega el Tribunal de Cuentas Europeo (TCE), institución encargada de la fiscalización de la gestión financiera de la Unión Europea (UE) y que cristaliza la línea que ha seguido la UE en esta materia. Dicho organismo define la ciberseguridad como "*todas las salvaguardas y medidas adoptadas para defender los sistemas de información y sus usuarios contra accesos no autorizados, ataques y daños, para garantizar la confidencialidad, integridad y disponibilidad de datos*".[13]

Asimismo, el TCE establece a este respecto que la ciberseguridad involucra prevenir, detectar, responder y recuperarse de incidentes cibernéticos, los cuales están dados por cualquier actividad ilegal que implique el uso de tecnologías digitales en el ciberespacio.[14]

---

[11] Ibid.
[12] Sancho Hirane, "Ciberinteligencia: Contextualización, Aproximación Conceptual, Características y Desafíos", 3.
[13] "Challenges to effective EU cybersecurity policy", *European Court of Auditors*, marzo 2019, en línea, consulta: 2 de septiembre de 2019, disponible: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.
[14] Ibid.

Por ende, se da una definición amplia de este concepto, cuestión que resulta fundamental debido a la naturaleza de la materia de la que se trata, lo que será expuesto con mayor profundidad más adelante. Dicha amplitud permite a los diferentes ordenamientos jurídicos dotar de las herramientas necesarias a sus instituciones para el combate del cibercrimen, tomando en consideración las diferencias culturales y de dotación técnica entre los Estados.

1.3 Ciberdelito

Para este concepto, ocuparemos la definición propuesta por la Dirección General de Migración y Asuntos Interiores de la Unión Europea, según la cual los ciberdelitos son "*aquellos actos delictivos que se cometen en línea mediante el uso de redes de comunicaciones electrónicas y sistemas de información*".[15] Se trata de un problema "sin fronteras", el cual podemos clasificar en tres amplias categorías:[16]

a. Delitos específicos de Internet, como ataques contra sistemas de información o suplantación de identidad.
b. Fraude y falsificación en línea.
c. Contenido ilegal en línea, incluido material de abuso sexual infantil, incitación al odio racial, incitación a actos terroristas y glorificación de la violencia, el terrorismo, el racismo y la xenofobia.

Siguiendo esta clasificación, y a modo meramente ilustrativo, los delitos que contempla expresamente el Convenio de Budapest son: acceso ilícito, interceptación ilícita, ataques a la integridad de datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones a la propiedad intelectual y a los derechos afines.

No obstante, si bien es posible dar una descripción precisa de los diversos tipos de delitos informáticos, no ha sido posible proporcionar una estimación precisa del alcance de las pérdidas que ocasionan y del número real de ciberdelitos. La cantidad de estos crímenes que permanecen ocultos, porque no se denuncian o se desconocen, se puede atribuir a las

[15] "Cybercrime", *Migration and Home Affairs European Commission*, en línea, consulta: 3 de septiembre de 2019, disponible: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime.
[16] Ibid.

siguientes razones:[17]

a. Se utiliza tecnología de información y comunicaciones de alto nivel.
b. Los investigadores de estos delitos no se encuentran suficientemente capacitados.
c. Se desconoce la identidad de la totalidad de los afectados.
d. En el caso de empresas, se produce una resistencia por parte de las víctimas a denunciar delitos cibernéticos, por miedo a una mala publicidad.

2. Carácter transfronterizo de los ciberdelitos y desafíos a la hora de legislar

En el caso de los hechos ilícitos de carácter cibernético, es muy habitual encontrarse con conductas que presentan un carácter transfronterizo y/o extraterritorial, cuestión que ha permitido que en muchas ocasiones se cometan delitos en los cuales los culpables no pueden ser perseguidos con la celeridad que este tipo de actos requiere. Se trata de acciones que suponen un quiebre en el esquema jurídico tradicional, puesto que por su peculiar forma de ejecución es perfectamente posible que se cometan hechos ilegales en un punto del planeta y que se produzcan los resultados en otro lugar distinto, o incluso que se cometan simultáneamente en diferentes territorios, a veces muy distantes entre sí. En consecuencia, dado que la naturaleza de los ciberdelitos es global, la respuesta a estos también debería serlo.[18]

Lo anterior ha sido objeto de un fuerte debate en el último tiempo, tanto a nivel legislativo como académico, puesto que se trata de una cuestión que pone en tela de juicio el principio de territorialidad penal consagrado en las diferentes jurisdicciones. Ello, por cuanto la realidad criminal más importante a nivel internacional se desarrolla en un lugar indeterminado llamado ciberespacio, con unas coordenadas temporales y espaciales difíciles de aprehender.[19] Es por esto que, pese a las dificultades técnicas que esta materia supone a la hora de establecer normas, tanto de carácter sustantivo como procedimental, resulta imperativo contar con una legislación que permita una correcta investigación por parte de las

[17] Cerezo, Lopez y Patel, "International Cooperation to Fight Transnational Cybercrime", 15.
[18] Dogrul, Aslan y Celik, "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", 36.
[19] María Concepción Rayón y José Antonio Gómez, "Cibercrimen: particularidades en su investigación y enjuiciamiento", *Anuario Jurídico y Económico Ecurialense* XLVII (2014), 233.

autoridades policiales y judiciales de cada país afectado por un delito cibernético.[20] En otras palabras, una normativa moderna debiese sentar las bases para facilitar la cooperación entre los Estados afectados con miras a la persecución de estos delitos.

A nivel internacional, la ciberseguridad se enfrenta a múltiples desafíos, los cuales se complejizan con la integración mundial que produce la globalización. Numerosos autores han determinado la existencia de diversas amenazas para la seguridad nacional que se originan en el ciberespacio, entre ellos, el ciberterrorismo, el cibercrimen y el ciberespionaje.[21] Sin embargo, a nivel de derecho internacional, no se han hecho los esfuerzos normativos suficientes para combatir cada una de dichas amenazas, a excepción del Convenio de Budapest. En la práctica, los Estados han considerado suficiente recurrir a normas convencionales o consuetudinarias ya vigentes en instrumentos internacionales, haciendo una aplicación extensiva de ellas, con el fin de responder a estos desafíos.[22] No obstante lo anterior, resulta evidente que esta solución es completamente anacrónica e insuficiente, siendo fundamental en esta materia que los diferentes Estados cuenten con leyes armónicas que permitan salvar esta situación y faciliten un entendimiento común a la hora de investigar cibercrímenes.[23]

Existen numerosas dificultades a la hora de idear leyes que permitan una adecuada persecución de delitos que se perpetran utilizando nuevas tecnologías, no solo a la hora de su investigación, sino también al momento de ser enjuiciados. Al respecto, la profesora María Concepción Rayón, de la Universidad Complutense de Madrid, enlista de forma muy clara cuáles son los principales desafíos a los que se enfrentan los ordenamientos jurídicos en esta materia, siendo los más importantes los siguientes:[24]

a. <u>La tecnología facilita la perpetración de nuevas conductas dañosas y la ocultación de los rastros de estas</u>. Es una realidad innegable que el mundo digital avanza a un ritmo mucho más rápido que la normativa que lo trata de regular. Es por esto que la

[20] Ibid.
[21] Antonio Segura, "Ciberseguridad y derecho internacional", *Revista Española de Derecho Internacional* 69, no. 2 (Madrid, 2017), 293.
[22] Ibid.
[23] Cerezo, Lopez y Patel, "International Cooperation to Fight Transnational Cybercrime", 15.
[24] Rayón y Gómez, "Cibercrimen: particularidades en su investigación y enjuiciamiento", 230.

capacidad del legislador de comprender los alcances y dinámicas del mundo digital resulta insuficiente, lo que conlleva la existencia de vacíos legales y espacios de impunidad respecto a ciberdelitos, cuestión que resulta especialmente compleja de abordar en las diferentes instancias legislativas.[25]

b. La tipificación de las conductas resulta complicada, pues muchas veces los hechos son tan novedosos que no están contemplados en las normas penales. Es por lo anterior que para poder perseguir delitos cibernéticos resulta imprescindible contar con leyes flexibles y dinámicas, que permitan adaptarse a las diversas formas que esta clase de ilícitos puede adoptar. En otras palabras, las normas que regulen la ciberseguridad deben evitar definiciones rígidas y excesivamente descriptivas, estableciendo tipos penales abiertos que permitan una persecución efectiva ante una acción dañosa que cumpla con los requisitos establecidos en la misma ley, cualquiera sea su índole o canal de ejecución.[26]

c. En la investigación de este tipo de delitos resulta frecuente que el autor se enmascare bajo identidades falsas a través de la utilización de apodos, *nicks* o suplantaciones de identidad. Este punto es de particular interés para el motivo del presente trabajo, ya que, aprovechándose de esto, el autor de un ciberdelito puede ocultar su identidad al momento de cometer diferentes ilícitos, utilizando servidores cruzados localizados en diversas jurisdicciones, haciendo casi imposible determinar su ubicación concreta. Lo anterior, sumado a la comisión a distancia mediante la cual normalmente se ejecutan este tipo de crímenes, produce que estos alcancen muchos países al mismo tiempo de forma instantánea, masiva y altamente dañina.[27]

d. En este tipo de acciones, la extraterritorialidad juega frecuentemente un rol preponderante, lo que conlleva problemas de jurisdicción, de operatividad policial y judicial, y de determinación de la ley y del procedimiento aplicable.[28]

Es por todos estos motivos, entre muchos otros, que el problema de la ciberseguridad requiere

[25] Ibid.
[26] Ibid.
[27] Ibid., 231.
[28] Ibid., 232.

ser tratado desde una mirada internacional. La respuesta por parte de las autoridades de un país a este tipo de crímenes no puede estar limitada por las fronteras físicas de los Estados, cuestión que, como ya hemos establecido, puede provocar la creación de un grave espacio de impunidad para esta clase de ilícitos. Por el contrario, el apoyo y cooperación de los diferentes miembros de la comunidad internacional resulta imprescindible para poder hacer frente a la ciberdelincuencia, estrechando los esfuerzos de los diferentes países en esta materia y armonizando las normativas locales que regulan el ciberespacio.

3. El principio de cooperación jurídica internacional

3.1 Concepto

Según lo establecido por la Agencia Chilena de Cooperación Internacional para el Desarrollo (AGCID), el principio general de cooperación internacional se define como "*la relación que se establece entre dos o más países, organismos u organizaciones de la sociedad civil, con el objetivo de alcanzar metas de desarrollo consensuadas. También se refiere a todas las acciones y actividades que se realizan entre naciones u organizaciones de la sociedad civil tendientes a contribuir con el proceso de desarrollo de las sociedades de países en vías de desarrollo*".[29]

En base a lo anterior, podemos afirmar que la cooperación internacional —en términos generales— es el instrumento mediante el cual los diferentes miembros de la comunidad internacional materializan los principios de solidaridad entre los pueblos, respeto y protección de los derechos humanos. Se basa en la búsqueda de una mejor calidad de vida para todas las personas, que les brinde una situación de bienestar conforme a su dignidad humana.[30]

De este principio general de cooperación internacional se desprende uno de aplicación específica en materia legislativa, denominado *principio de cooperación jurídica*

[29] "¿Qué es la cooperación?", *Agcid Chile*, en línea, consulta: 20 de septiembre de 2019, disponible: https://www.agci.cl/que-es-la-cooperacion.
[30] Morillo, Javier, ed. "La cooperación internacional y el derecho", en: *La cooperación internacional y su régimen jurídico en Colombia.* Bogotá: Agencia Presidencial para la Acción Social y la Cooperación Internacional, 2008, 11.

internacional. En palabras de la renombrada jurista Ana Elizabeth Villalta —miembro actual del Comité Jurídico Interamericano (CIJ)—[31] "*la cooperación jurídica internacional es la colaboración o asistencia legal mutua entre Estados, con el objeto de practicar las diligencias que sean necesarias en el desarrollo de un proceso que se ventila en el territorio de otro Estado*".[32] La finalidad de este principio es lograr una armonización entre las legislaciones y procedimientos de los diferentes Estados, de modo tal que se eliminen barreras y obstáculos innecesarios para poder regular materias de carácter internacional de forma eficaz, eficiente y expedita.[33]

3.2 Importancia

Producto de factores tales como la globalización, el crecimiento de los procesos de integración regional y la masificación de los medios de comunicación, han surgido una serie de asuntos jurídicos transfronterizos que exigen encontrar soluciones legislativas al alero del principio de cooperación jurídica internacional.[34] Ningún Estado de forma individual puede abordar adecuadamente los desafíos globales que enfrenta la comunidad internacional moderna, independientemente de cuán poderoso sea dicho actor. Ya sea que se piense en el cambio climático, el terrorismo internacional o las amenazas cibernéticas, todos los fenómenos contemporáneos necesitan un marco para la cooperación internacional.[35] Así, la importancia de la cooperación jurídica internacional recae, en que a través de un trabajo estrechamente coordinado entre instituciones policiales y judiciales pertenecientes a diferentes ordenamientos jurídicos, se pueden maximizar recursos que, de otra forma, se perderían en un esfuerzo inútil debido a la incapacidad técnica que cada legislación enfrenta de forma aislada.[36] Lo anterior ha sido reconocido —al menos en teoría— por uno de los tres principios sobre los cuales se erige la política exterior chilena, a saber, el principio de la

[31] "Comité Jurídico Interamericano CIJ | Misión Permanente de Colombia ante la OEA," n.d., en línea, consulta: 9 de septiembre de 2019, disponible: https://washington-oea.mision.gov.co/comite-juridico-interamericano-cij.
[32] Ana Elizabeth Villalta Vizcarra, "Cooperación jurídica internacional en materia civil y penal", *Rev. secr. Trib. perm. revis.* 5, no. 10 (2017), 102.
[33] Ibid.
[34] Ibid.
[35] Kubo Macak, "Is the International Law of Cyber Security in Crisis?", *8th International Conference on Cyber Conflict* (Tallinn, 2016), 128.
[36] Rayón y Gómez, "Cibercrimen: particularidades en su investigación y enjuiciamiento", 233.

responsabilidad de cooperar.[37]

En concreto, los problemas relacionados con la ciberseguridad son cuestiones a las cuales se enfrentan de forma transversal todos los países del mundo. En ese sentido, la cooperación entre diferentes Estados para perseguir este tipo de delitos y consagrar un marco normativo que permita eliminar los espacios de impunidad que actualmente existen es absolutamente fundamental.[38] En suma, la importancia de la cooperación internacional en esta área se traduce en la transferencia de experiencias y conocimientos adquiridos por los diferentes Estados al momento de enfrentarse a hechos ilícitos ocurridos en el ciberespacio, lo que sin lugar a duda contribuye a un fortalecimiento global de la lucha contra la ciberdelincuencia.

3.3 Recepción en el derecho internacional

La primera gran manifestación general del principio de cooperación internacional se encuentra en el Capítulo IX ("*Cooperación Internacional Económica y Social*") de la Carta de las Naciones Unidas (1945).[39] Dicho instrumento establece en su artículo 55 que "*con el propósito de crear las condiciones de estabilidad y bienestar necesarias para las relaciones pacíficas y amistosas entre las naciones, basadas en el respeto al principio de la igualdad de derechos y al de la libre determinación de los pueblos, la Organización promoverá: […] (b) La solución de problemas internacionales de carácter económico, social y sanitario, y de otros problemas conexos; y la cooperación internacional en el orden cultural y educativo*". Luego, su artículo 56 señala que "*todos los Miembros se comprometen a tomar medidas conjunta o separadamente, en cooperación con la Organización, para la realización de los propósitos consignados en el Artículo 55*". Así, la Carta regula el principio de cooperación internacional como un mandato para todos los miembros de la ONU y que rige cualquier asunto que pueda suscitarse entre ellos en materia económica, social, sanitaria u otras.

Este principio también se encuentra recogido en términos generales en la Carta de la

[37] "Ministerio de Relaciones Exteriores de Chile - Principios de la Política Exterior Chilena," n.d., en línea, consulta: 9 de septiembre de 2019, disponible: https://minrel.gob.cl/principios-de-la-politica-exterior-chilena/minrel/2008-08-02/194424.html#vtxt_cuerpo_T2.
[38] Villalta Vizcarra, "Cooperación jurídica internacional en materia civil y penal", 100.
[39] Organización de las Naciones Unidas, "*Carta de las Naciones Unidas*", 24 de octubre de 1945, disponible: https://www.un.org/es/charter-united-nations/.

Organización de Estados Americanos (1948),[40] particularmente en su artículo 3, que señala que "*los Estados americanos reafirman los siguientes principios: […] e) Todo Estado tiene derecho a elegir, sin injerencias externas, su sistema político, económico y social, y a organizarse en la forma que más le convenga, y tiene el deber de no intervenir en los asuntos de otro Estado. Con sujeción a lo arriba dispuesto, los Estados americanos cooperarán ampliamente entre sí y con independencia de la naturaleza de sus sistemas políticos, económicos y sociales*".

Como es evidente, ambas Cartas —tanto la de la ONU como la de la OEA— recogen el principio de cooperación internacional de forma amplia y general en un contexto de relaciones internacionales multilaterales. Por ello, resulta importante destacar, para efectos de poder analizar el principio de cooperación jurídica internacional en el contexto específico de la ciberseguridad, que el derecho internacional moderno se concibe como un derecho constituido por numerosas ramas especializadas que emergen de un núcleo común.[41] En este sentido, hoy nos encontramos con el Derecho Internacional de los Derechos Humanos, el Derecho Penal Internacional, el Derecho Humanitario, el Derecho del Mar, el Derecho del Medio Ambiente, el Derecho Mercantil, entre otros. Consecuentemente, muchas reglas y principios que forman parte del régimen internacional general tienen una aplicación matizada dependiendo de la rama específica en la que se encuentren circunscritos. Es por ello que, si bien existe un principio de cooperación internacional general, recogido por las Cartas de las principales organizaciones internacionales, dicho principio también se encuentra recogido de forma específica en numerosos instrumentos internacionales propios de cada una de las ramas especializadas del derecho internacional.[42]

En este sentido, el principio de cooperación jurídica internacional constituye una manifestación del principio general de cooperación internacional en instrumentos bilaterales y multilaterales celebrados entre Estados que versan sobre materias particulares. A juicio de

[40] Organización de los Estados Americanos, "*Carta de la Organización de los Estados Americanos*", 1948, disponible: http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A-1_carta_OEA.asp.
[41] Mauricio Hedocia, "Los Principios de Derecho Internacional Contenidos en la Carta de la OEA", n.d., en línea, consulta: 29 de agosto de 2019, disponible: https://www.oas.org/dil/esp/XXXVIII_Curso_Derecho_Internacional_principios_derecho_internacional_carta_OEA_mauricio_herdocia.pdf.
[42] Véanse *los Principios Fundamentales del Movimiento de la Cruz Roja y de la Media Luna Roja*. Véase el Principio 7mo de la *Declaración de Río sobre el Medio Ambiente y el Desarrollo*. Véase también el preámbulo del *Estatuto de Roma*.

la ya citada jurista del Comité Jurídico Interamericano Ana Elizabeth Villalta, "*la cooperación jurídica internacional se fundamenta preferentemente en los instrumentos internacionales bilaterales o multilaterales, y, a falta de éstos, deben aplicarse los Principios de Cooperación Judicial, la legislación interna del Estado requerido y de manera especial el Principio de Reciprocidad*".[43] Además, cabe mencionar entre algunos de los instrumentos que consagran el principio de cooperación jurídica internacional la Convención Interamericana sobre Asistencia Mutua en Materia Penal,[44] los tratados bilaterales de extradición celebrados entre la República de Chile y otros Estados[45] y, finalmente, el propio Convenio de Budapest.

En los siguientes capítulos, se abordará tanto la manera en que ha sido consagrado el principio de cooperación jurídica internacional en los diferentes instrumentos jurídicos internacionales, como su recepción en la legislación chilena actualmente vigente.

[43] Villalta Vizcarra, "Cooperación jurídica internacional en materia civil y penal", 103.
[44] Organización de los Estados Americanos, "Convención Interamericana sobre Asistencia Mutua en Materia Penal", 23 de mayo de 1992, en línea, consulta: 10 de septiembre de 2019, disponible: https://www.oas.org/juridico/spanish/tratados/a-55.html.
[45] Véase el Acuerdo sobre Extradición entre el MERCOSUR, La República de Bolivia y la República de Chile; el Tratado de Extradición entre el Gobierno de la República de Chile y el Gobierno de la República de los Estados Unidos de América; el Tratado de Extradición entre Chile y Perú; y el Tratado de Extradición entre Chile y Colombia.

CAPÍTULO II: NORMATIVA INTERNACIONAL EN MATERIA DE CIBERSEGURIDAD

1. Antecedentes históricos

Según un estudio publicado en la Revista Latinoamericana de Estudios de Seguridad, Internet nació en el año 1969, luego de los avances tecnológicos desarrollados durante la guerra fría por el *Advanced Research Projects Agency* (ARPA) de EE. UU.[46] Desde entonces, el número de usuarios de dicha plataforma ha ido aumentando de forma exponencial, especialmente a partir de la década de los noventa.[47] Asimismo, se estima que, desde el año 2000 al 2008, a nivel mundial Internet se expandió en un 305% en promedio[48] y, según estadísticas de la Unión Internacional de Telecomunicaciones (UIT), para fines del año 2019, el 53.6% de la población mundial (4.1 billones de personas) sería usuario de Internet.[49] Este es el escenario en el que han ido surgiendo —cada vez con mayor frecuencia— los ciberdelitos y, como respuesta a ellos, los tratados internacionales que los intentan regular.

El primer gran ciberataque se remonta a fines de la década de los ochenta, cuando computadoras de la NASA fueron atacadas por un virus llamado *WANK worm* que entorpeció su funcionamiento regular en 1989.[50] A este ataque le siguieron incidentes tales como el "*netstrike*", efectuado en contra del gobierno francés en 1995, la disrupción en el funcionamiento corriente de las páginas web del Pentágono por parte del *Electronic Disturbance Theater* en 1998 y las protestas virtuales llevadas a cabo por el *Team Spl0it*, llamando al fin del conflicto en Kosovo en 1999, entre otros.[51] Si bien estos primeros ciberataques fueron llevados a cabo por pequeños grupos privados y no generaron

[46] Vicente Pons Gamon, "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity", *URVIO. Revista Latinoamericana de Estudios de Seguridad* 20 (2017), 80–93.
[47] Banco Mundial, "Personas que usan Internet (% de la población) | Data" (n.d.), online, consulta: 25 de septiembre de 2019, disponible: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS.
[48] Stein Schjolberg, "The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva", *Journal of International Commercial Law and Technology* 1, no. 12 (2008), 1.
[49] "Statistics", *International Telecommunication Union,* en línea, consulta: 2 de marzo de 2020, disponible: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
[50] Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis y Theodorus Apostolopoulos, "Cyberoperations and international humanitarian law", *Information & Computer Security* (2016), en línea, consulta: 25 de septiembre de 2019, disponible: https://www.emerald.com/insight/content/doi/10.1108/ICS-12-2014-0081/full/html.
[51] Thomas Berson y Dorothy Denning, "Cyberwarfare", *IEEE Security & Privacy* 9 (2011), 13–15.

consecuencias de grandes magnitudes, sí marcaron el punto de partida de las primeras discusiones entre Estados sobre las repercusiones de las ciberoperaciones en las relaciones internacionales y la necesidad de regularlas universalmente.[52] A raíz de lo anterior fue que comenzó la codificación, en diversos instrumentos internacionales, del derecho internacional aplicable en materia de ciberseguridad, la cual a la fecha sigue en constante expansión y desarrollo.

2. Instrumentos internacionales relevantes

Producto de los antecedentes mencionados en el apartado anterior —que, por cierto, solamente dan cuenta de una pequeña muestra de los hitos generadores de las discusiones que eventualmente culminaron con la entrada en vigor de la normativa que actualmente regula la ciberseguridad—, han nacido numerosos instrumentos internacionales de diversa naturaleza jurídica. Teniendo ello en cuenta, debemos hacer énfasis en que esta sección únicamente se ocupará de analizar aquellos que han ejercido una mayor influencia en la normativa interna de ciberseguridad de los Estados. Entre la normativa internacional más relevante sobre ciberseguridad cabe examinar, en primer lugar, el Convenio de Budapest o Convenio sobre la ciberdelincuencia (2001); en segundo lugar, el Manual de Tallin 2.0 sobre el derecho internacional aplicable a la guerra cibernética (2017); y, en tercer lugar, el Reglamento General de Protección de Datos de la Unión Europea (2018).

2.1 Convenio de Budapest

El Convenio sobre la ciberdelincuencia, conocido popularmente como Convenio de Budapest, es el único instrumento internacional vigente a la fecha que aborda materias de ciberseguridad de forma específica.[53] Este tratado nació con el objeto de contrarrestar las amenazas que fueron surgiendo en el contexto internacional a raíz del sostenido desarrollo de la tecnología computacional. Específicamente, su objetivo se centra en luchar contra la impunidad de los diversos delitos cometidos en el ciberespacio, a través de la armonización

[52] Pipyros, Mitrou, Gritzalis y Apostolopoulos, "Cyberoperations and international humanitarian law", 39.
[53] Asociación por los Derechos Civiles, "La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas", marzo 2018, disponible: https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf.

de la normativa de los Estados en torno a su regulación.[54] Para estos efectos, en 1997 el Consejo de Europa (COE, por sus siglas en inglés) designó a un comité de expertos para el desarrollo de un instrumento que facilitara la cooperación internacional en materia de investigación y persecución de ciberdelitos.[55] En junio de 2001, dicho comité presentó una versión final del Convenio, la cual luego fue abierta el 23 de noviembre de 2001 para su suscripción, precisamente en la ciudad de Budapest.[56] Tras aproximadamente dieciocho años desde su entrada en vigor, en la actualidad el Convenio cuenta con 64 Estados miembros que lo han firmado y ratificado, nueve Estados observantes y once organizaciones observantes al comité del Convenio.[57]

En cuanto a su estructura normativa, el Convenio está compuesto por 48 artículos, los cuales se encuentran divididos en cuatro capítulos, cada cual con sus respectivas secciones. El primer capítulo, titulado "*Terminología*", define ciertos conceptos claves de la disciplina, con el objeto de lograr un correcto entendimiento de estos en los artículos en que se emplean. El segundo capítulo, denominado "*Medidas que deberán adoptarse a nivel nacional*", establece diversas cuestiones que deben ser implementadas por los Estados miembros en su derecho interno para dar cumplimiento al Convenio. Este capítulo se encuentra dividido a su vez en dos secciones: una primera relativa al "*derecho penal sustantivo*", en donde se estipula el deber de criminalizar ciertas conductas realizadas mediante dispositivos tecnológicos, y una segunda relativa al "*derecho procesal*", en donde se establece la necesidad de adoptar ciertas medidas en relación con el procedimiento de investigación. El tercer capítulo, titulado "*Cooperación internacional*", fija ciertas reglas de cooperación mutua entre Estados respecto a diversas materias, entre ellas, la extradición, los intercambios de información, la conservación rápida de datos informáticos almacenados, entre otras. Finalmente, el cuarto capítulo, titulado "*Cláusulas finales*", trata sobre cuestiones referentes al tratado en sí, tales como su firma y entrada en vigor, su aplicación territorial, sus efectos, las reservas que pueden formularse, los mecanismos de solución de controversias, consultas entre las partes,

[54] Susan Brenner, "La Convención sobre Cibercrimen del Consejo de Europa", *Revista Chilena de Derecho y Tecnología* 1, no. 1 (2012), 221–238.
[55] "Adoption of Convention on Cybercrime", *The American Journal of International Law* 95, no. 4 (2001), pp. 889–891, en línea, consulta: 1 de octubre de 2019, disponible: www.jstor.org/stable/2674643.
[56] Brenner, "La Convención sobre Cibercrimen del Consejo de Europa", 222.
[57] "Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY", n.d., en línea, consulta: 30 de septiembre de 2019, disponible: https://www.coe.int/en/web/cybercrime/parties-observers.

entre otros temas.[58]

Dentro de los delitos que el Convenio exige que las partes criminalicen en su derecho interno de manera universal, encontramos a grandes rasgos los siguientes: (i) actividades que tienen como blanco los sistemas informáticos y la data; (ii) la falsificación informática; (iii) los fraudes informáticos; (iv) el uso de la tecnología computacional para la creación, distribución y procesamiento de pornografía infantil; y (v) el uso de la tecnología computacional para infringir reglas relativas a la propiedad intelectual.[59] Luego, en lo relativo a las medidas que el Convenio busca que los Estados parte adopten para lograr una investigación más expedita y eficaz de los delitos mencionados, aquel requiere que los Estados adopten una legislación que permita: (i) la preservación y producción de evidencia electrónica; (ii) la búsqueda e incautación legal de sistemas informáticos; y (iii) la recolección de datos de tráfico y de contenido por parte de las autoridades. Para ello, se exige que las partes colaboren en las siguientes materias: (i) la extradición de los delincuentes; (ii) el intercambio de información; y (iii) la preservación, acceso, interceptación y relación de datos de tráfico y contenido, asignando un punto de contacto que sea responsable de asegurar una asistencia inmediata en investigaciones y procedimientos relacionados a los ciberdelitos.[60]

Conforme a lo señalado en el "*Informe Explicativo*" del Convenio, aprobado por el Comité de Ministros del Consejo de Europa, sus finalidades primordiales son: "*1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos; 2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentran en formato electrónico, y 3) establecer un régimen rápido y eficaz de cooperación internacional*".[61] Sin embargo, para que el Convenio logre cumplir plenamente con estos objetivos, no basta con el mero hecho de que los Estados lo firmen y ratifiquen, sino que además deben adoptar las medidas necesarias

[58] Consejo de Europa, "Convenio sobre la Ciberdelincuencia", 23 de noviembre de 2001, en línea, consulta:5 de octubre de 2019, disponible: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf.
[59] Brenner, "La Convención sobre Cibercrimen del Consejo de Europa", 227.
[60] Ibid., 229.
[61] Consejo de Europa, "Informe Explicativo del Convenio sobre la ciberdelincuencia", 8 de noviembre de 2001, en línea, consulta: 5 de octubre de 2019, disponible: https://rm.coe.int/16802fa403.

para incorporar sus mandatos a nivel interno.[62] De lo contrario, este no lograría surtir plenos efectos, pues la mayoría de las normas que contempla son *non-self-executing norms*, es decir, son disposiciones que por sí solas no son suficientemente completas como para ser aplicadas internamente y, por ende, requieren la dictación de medidas legislativas o reglamentarias que las desarrollen.[63] En consecuencia, la efectividad de la normativa contemplada en el Convenio de Budapest dependerá, últimamente, de la voluntad de los Estados que lo suscriban de incorporar sus mandatos a nivel interno.

2.2 Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas

Un hito que marcó un verdadero punto de inflexión en la discusión en torno al impacto de las ciberoperaciones en el derecho internacional fue el ciberataque llevado a cabo en Estonia el año 2007, el cual dio lugar a la creación del Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN y la posterior publicación de las versiones 1.0 y 2.0 del Manual de Tallin sobre el derecho internacional aplicable a las operaciones cibernéticas.[64] En abril del 2007, la polémica decisión del gobierno estonio de trasladar una estatua de un soldado soviético a las afueras de la capital desencadenó una serie de arduas protestas en las calles, que luego se trasladaron al espacio virtual.[65] Organismos públicos, bancos, periódicos y otras entidades privadas fueron víctimas de uno de los mayores ciberataques registrados en la historia, el cual causó el colapso de la red virtual prácticamente completa de uno de los países más digitalizados del mundo.[66] Este hecho fue particularmente relevante, dado que causó que la comunidad internacional se percatara de dos cuestiones fundamentales en materia de ciberseguridad: la primera, que mientras más digitalizado se encuentre un Estado, mayor es el riesgo de que el mismo sea blanco de ciberataques o ciberdelitos, y la segunda, que existía

[62] Brenner, "La Convención sobre Cibercrimen del Consejo de Europa", 235.
[63] Santiago Benadava, "Las relaciones entre derecho internacional y derecho interno ante los tribunales chilenos", en *Nuevos enfoques del derecho internacional*, coord. Avelino León (Santiago, Chile: Editorial Jurídica de Chile, 1992), 42.
[64] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Reino Unido: Cambridge University Press, 2017).
[65] Damien McGuinness, "How a cyber-attack transformed Estonia", *BBC News*, 27 de abril de 2017, sec. Europe, en línea, consulta: 5 de septiembre de 2019, disponible: https://www.bbc.com/news/39655415.
[66] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired*, 21 de agosto de 2007, en línea, consulta: 16 Sep. 2019, disponible: https://www.wired.com/2007/08/ff-estonia/.

un enorme vacío respecto a la aplicabilidad de las normas internacionales generales en materia de ciberoperaciones (como, por ejemplo, la aplicación del *jus ad bellum* en materias de ciberseguridad).[67]

A propósito de este suceso, la OTAN abrió en el año 2008 su Centro de Excelencia para la Ciberdefensa Cooperativa en Tallin, institución destinada a la investigación multidisciplinaria de asuntos relacionados con el derecho de las operaciones cibernéticas.[68] Tras un año desde su constitución, en 2009, el Centro convocó a un grupo de expertos independientes para elaborar un manual sobre el derecho internacional aplicable a las ciberoperaciones. El proyecto reunió a numerosos académicos y autoridades expertas en materias de ciberseguridad para examinar cómo aplicar el derecho internacional existente a las operaciones que tienen lugar en el ciberespacio. El resultado de este trabajo fue el Manual de Tallin 1.0 sobre el derecho internacional aplicable a las operaciones cibernéticas, del año 2013. Luego de su publicación, el Centro de Excelencia para la Ciberdefensa Cooperativa convocó a un segundo grupo de expertos para que expandieran el trabajo realizado por el primero, lo que culminó con la publicación de la versión 2.0 del Manual en el año 2017, su versión más completa y actualizada a la fecha.[69]

A diferencia de tratados internacionales como el Convenio de Budapest, el Manual de Tallin 2.0 no es un documento vinculante para los Estados. No obstante lo anterior, se trata de un texto de suma relevancia, dado que da cuenta de la doctrina acordada por los especialistas de mayor competencia de las distintas naciones, lo cual, conforme a lo señalado en el artículo 38 del Estatuto de la Corte Internacional de Justicia, constituye una fuente subsidiaria de derecho internacional.[70] El objetivo del Manual consiste en desarrollar —en forma de *lege lata*— cuál sería el derecho internacional aplicable a las ciberoperaciones a juicio del grupo

[67] María Pilar Llorens, "Los desafíos del uso de la fuerza en el ciberespacio", *Anuario Mexicano de Derecho Internacional* 1, no. 17 (2017), 785–816.
[68] "CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.," n.d., en línea, consulta: 1 de octubre de 2019, disponible: https://ccdcoe.org/.
[69] Véase la introducción al International Group of Experts at the NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*.
[70] Organización de las Naciones Unidas, "Estatuto de la Corte Internacional de Justicia," 1945, disponible: https://www.icj-cij.org/files/statute-of-the-court/statute-of-the-court-es.pdf.Art. 38 (1) (d).

de expertos.[71] Para ello, los especialistas convocados han elaborado un conjunto de reglas aplicables a diversas materias de derecho internacional, junto con comentarios que ahondan sobre la aplicación de las mismas. De esta forma, este documento procura brindar asistencia legal a los asesores jurídicos de los Estados respecto de diversos temas que pueden ser relevantes a la hora de elaborar un proyecto de ley aplicable a las ciberoperaciones en sus respectivos Estados.[72] En consecuencia, el Manual es un texto de suma utilidad para aquellos Estados que buscan desarrollar por primera vez un marco normativo interno aplicable a la ciberseguridad, o bien, para aquellos que buscan robustecer su normativa existente.

2.3 Reglamento General de Protección de Datos de la Unión Europea

El Reglamento General de Protección de Datos de la Unión Europea es un instrumento regional que busca cristalizar el derecho fundamental a la protección de datos de carácter personal, contemplado tanto en la Carta de Derechos Fundamentales de la UE como en el Tratado de Funcionamiento de la misma organización.[73] Se trata de un reglamento que armoniza las normas de protección de datos de todos los países de dicho organismo internacional y que, en consecuencia, eleva los estándares aplicables al resto del mundo con el objeto de proteger al usuario europeo frente al mal uso de sus datos.[74] Este reglamento fue aprobado por el Parlamento de la UE el 14 de abril de 2016 y entró en vigencia el 25 de mayo de 2018.[75]

En sus considerandos, el Reglamento expresa que "*[…] las transferencias [de datos personales] a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o*

[71] International Group of Experts at the NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, 3.
[72] Ibid.
[73] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento General de Protección de Datos de la UE" (Diario Oficial de la Unión Europea, abril 2016), disponible: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679. Considerando Nº1.
[74] PricewaterhouseCoopers, "¿Cómo afecta a Chile el nuevo Reglamento General de Protección de Datos de la UE?", n.d., en línea, consulta: 10 de octubre de 2019, disponible: https://www.pwc.com/cl/es/prensa/prensa/2018/Como-afecta-a-Chile-el-nuevo-Reglamento-General-de-Proteccion-de-Datos-de-la-UE.html.
[75] "EUGDPR – Information Portal", n.d., en línea, consulta: 22 de octubre de 2019, disponible: https://eugdpr.org/.

encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales".[76] Luego, su artículo tercero ("*Ámbito territorial*") señala expresamente que "*el presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independiente de que el tratamiento tenga lugar en la Unión o no*".[77] Por lo tanto, si bien se trata de un conjunto de reglas que en principio solo aplican a los miembros de la UE, estas podrían llegar a tener una aplicación extraterritorial sobre empresas y organizaciones que se encuentran fuera de los países que integran la Unión Europea[78] Dicha aplicación extraterritorial del Reglamento ha producido el impacto más importante de este a nivel mundial, debido a que altera los resguardos que deben tomar las empresas fuera del territorio de la UE respecto al procesamiento de datos de ciudadanos europeos. Lo anterior ha significado para muchos Estados fuera de la UE la necesidad de actualizar su marco jurídico aplicable a la protección de datos para cumplir con los estándares del Reglamento.[79]

3. Principio de cooperación jurídica en la normativa internacional sobre ciberseguridad

Si bien los textos aludidos en la sección anterior difieren drásticamente en cuanto a su naturaleza jurídica, todos tienen un elemento en común: incentivan a los Estados a legislar en materia de ciberseguridad, teniendo en cuenta el principio de cooperación jurídica internacional. En otras palabras, todos estos instrumentos promueven que los Estados cuenten con reglas uniformes y armónicas en materia de ciberseguridad, para así lograr una regulación más eficaz de esta tanto a nivel nacional como internacional.

En primer lugar, el Convenio de Budapest contempla este principio en su preámbulo como uno de los fundamentos del tratado, al señalar, entre otras cosas, lo siguiente: "*Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la*

[76] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento General de Protección de Datos de la UE", Considerando Nº 101.
[77] Ibid., art. 3.
[78] PricewaterhouseCoopers, "¿Cómo afecta a Chile el nuevo Reglamento General de Protección de Datos de la UE?".
[79] "EUGDPR – Information Portal".

confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable".[80] Cabe destacar aquí que lo establecido en el preámbulo de un tratado internacional es de suma relevancia, ya que allí se encuentran expresados el objeto y fin del tratado, según los cuales deben interpretarse sus normas, conforme al artículo 31 de la Convención de Viena sobre el Derecho de los Tratados.[81] Por consiguiente, una correcta lectura del Convenio de Budapest es aquella que se hace a la luz del principio de la cooperación jurídica internacional.

Por su parte, el Manual de Tallin 2.0 establece como criterio general que, si bien los Estados no tienen una obligación general de ayudarse mutuamente en la investigación y persecución de ciberdelitos, una cooperación de dicha naturaleza puede ser requerida por las reglas aplicables de un tratado internacional o de cualquier otra fuente de obligaciones internacionales.[82] En otras palabras, entre Estados que han suscrito tratados internacionales que contemplan obligaciones de cooperación jurídica en materia de ciberseguridad, existe un deber de legislar en miras de una persecución coordinada de los ciberdelitos. Lo anterior, sin lugar a duda, reafirma la importancia del principio de cooperación jurídica internacional entre Estados en lo relativo a la normativa internacional sobre ciberseguridad.

Finalmente, el Reglamento General de Protección de Datos de la UE establece en su considerando 10º que, "*para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento*

[80] Consejo de Europa, "Convenio sobre la Ciberdelincuencia", Preámbulo.
[81] Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), Judgement, ICJ Reports (2007).
[82] International Group of Experts at the NATO Cooperative Cyber Defence Centre of Excellence, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, Rule 13.

de datos de carácter personal sea coherente y homogénea".[83] Nuevamente, se deja en claro que una efectiva regulación de la ciberseguridad necesariamente debe realizarse conforme al principio de cooperación jurídica internacional.

Además de encontrarse recogido en el corazón de la normativa internacional aplicable a las ciberoperaciones, el principio de cooperación jurídica internacional también se vislumbra en la creciente creación de instrumentos y órganos especializados en materia de ciberseguridad a nivel regional en distintos continentes. Algunos ejemplos que reflejan esta tendencia son la recomendación de la OCDE titulada *Digital Security Risk Management for Economic and Social Prosperity*,[84] el G-8 *24/7 Network for Data Preservation* de la Organización de Estados Americanos,[85] la rama especializada de ciberseguridad de la Interpol[86] y el *Arab Regional Cybersecurity Center*.[87] Todos estos instrumentos y organismos especializados dan cuenta de la creciente necesidad de contar con reglas y autoridades especializadas a nivel regional, que unifiquen la regulación de la ciberseguridad y centralicen su funcionamiento, para así lograr una persecución más coordinada y eficaz del cibercrimen.

A partir del análisis realizado de la normativa internacional aplicable a la ciberseguridad, podemos establecer que todos los instrumentos internacionales vigentes —ya sean vinculantes jurídicamente o no para los Estados, ya se trate de instrumentos globales o regionales— dan cuenta de la necesidad de legislar la ciberseguridad en torno al principio de cooperación jurídica internacional para lograr una persecución verdaderamente eficaz del cibercrimen. Esto se debe a que toda la normativa internacional en materia de ciberseguridad nace a partir de un mismo presupuesto, esto es, que todos los Estados deben cooperar entre sí, debido a que el cibercrimen no se encuentra limitado por fronteras nacionales o geográficas, y la evidencia digital relativa a un delito puede encontrarse dispersada por

[83] Parlamento Europeo y Consejo de la Unión Europea, "Reglamento General de Protección de Datos de la UE", Considerando N.º 10.
[84] OECD, "Digital Security Risk Management for Economic and Social Prosperity" (OECD Publishing, Paris, 2015), en línea, consulta: 10 de octubre de 2019, disponible: http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.
[85] Albert Rees, "24/7 High Tech Crime Network" (2007), en línea, consulta: 10 de octubre de 2019, disponible: http://www.oas.org/juridico/english/cyb20_network_en.pdf.
[86] "Cybercrime," n.d., en línea, consulta: 24 de octubre de 2019, disponible: https://www.interpol.int/en/Crimes/Cybercrime.
[87] "Arab Regional Cyber Security Center," n.d., en línea, consulta: 24 de octubre de 2019, disponible: https://arcc.om/?GetLang=en.

múltiples regiones.[88] En conclusión, de conformidad con la normativa internacional vigente, un Estado regula eficazmente la ciberseguridad a nivel interno cuando su marco normativo se construye a partir de una base que reconoce la necesidad de cooperar jurídicamente a nivel internacional en esta materia.

[88] Cerezo, Lopez y Patel, "International Cooperation to Fight Transnational Cybercrime", 13.

CAPÍTULO III: NORMATIVA CHILENA EN MATERIA DE CIBERSEGURIDAD

Luego de estudiar la normativa que regula el ciberespacio a nivel de derecho internacional, procederemos a analizar cómo se ha regulado jurídicamente esta materia en nuestro país. Para estos efectos, se realizará un examen histórico sobre la legislación chilena de ciberseguridad y su estado actual, haciendo especial énfasis en la recepción del Convenio de Budapest en nuestro ordenamiento jurídico y finalizando con un breve comentario sobre la incorporación del principio de cooperación jurídica internacional en él.

1. Antecedentes históricos

"*Recuerdo que ocupaba toda una sala. Eran tres piezas del tamaño de un refrigerador o una lavadora*", cuenta Juan Álvarez, profesor del Departamento de Ciencias de la Computación de la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile. Álvarez no habla de un aparato de limpieza, sino del IBM 1401, el primer computador digital que llegó a Chile, en 1961.[89] Tuvieron que pasar 24 años para que, recién en 1985, se mandara el primer e-mail en nuestro país, el cual fue enviado por los ingenieros de la misma casa de estudios, José Miguel Piquer y Patricio Poblete. ¿Su contenido? "*Si este mail te llega, abramos una botella de champaña*".[90] En el caso de los teléfonos celulares, estos recién llegaron a comercializarse a Chile en 1988, año en el que el servicio contaba con solo tres antenas en Santiago, las cuales ofrecían toda la cobertura disponible.[91]

Estas anécdotas ilustran el desarrollo que tuvo el ciberespacio en nuestro país hasta comienzos de la década de 1990, época en la que, si bien el avance de la informática era cada vez mayor, aún no contábamos con ningún cuerpo legal que protegiera los datos que circulaban a diario por los diferentes sistemas de información. En otras palabras, nuestra normativa había quedado desfasada frente a un fenómeno que comenzó a dominar distintas esferas de nuestra vida cotidiana, tanto en el ámbito profesional como en el académico y el

[89] Axel Christiansen y Francisco Rodríguez, "La historia del primer computador que llegó a Chile", *La Tercera*, 17 de septiembre de 2019, en línea, consulta: 23 de septiembre de 2019, disponible: https://www.dcc.uchile.cl/sites/default/files/dcc_prensa/2010/0970_La%20Tercera_El%20primer%20computador.pdf.
[90] Ibid.
[91] Ibid.

personal.

En la actualidad, el panorama es radicalmente distinto. Según la IX Encuesta Acceso y Uso Internet, encargada en diciembre de 2017 por la Subsecretaría de Telecomunicaciones, el 87.4% de los hogares en Chile cuenta con acceso a Internet. En esa misma línea, otros estudios similares dan cuenta de que, entre 2013 y 2017, el índice de penetración de Internet en nuestro país aumentó en más de 9 millones de personas.[92]

Sin embargo, el explosivo aumento en el acceso al ciberespacio ha traído aparejada también una serie de consecuencias negativas, asociadas al mal uso que se les ha dado a las nuevas herramientas digitales. Es así como en los últimos años hemos sido testigos de una serie de ataques a bases informáticas de importantes empresas ligadas a industrias muy sensibles para la ciudadanía, como, por ejemplo, el mercado bancario. El 24 de mayo de 2018, usuarios del Banco de Chile reportaron problemas al acceder al sistema de banca en línea. Posteriormente, la institución confirmó el ciberataque, a través del cual se sustrajeron cerca de 10 millones de dólares.[93] Siguiendo la tónica de este tipo de delitos, y tras un estudio forense efectuado por Microsoft, se llegó a la conclusión que se estaba frente a un ataque internacional perpetrado por bandas criminales provenientes de Asia o Europa del Este.[94] Lo anterior confirma la necesidad de contar con herramientas de cooperación internacional que faciliten la persecución de delitos que, como vemos, son ejecutados en lugares remotos del planeta, pero que afectan directamente a nuestro país a través del ciberespacio.

A mayor abundamiento, según el Informe sobre las Amenazas para la Seguridad en Internet (ISTR) del 2019 elaborado por Symantec, en 2018 se produjeron 545.231 ataques por *ransomware* en 157 países alrededor del mundo, un programa de software malicioso que infecta los sistemas computacionales y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.[95] De las naciones que recibieron más ataques por

[92] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest*, 2018, en línea, consulta: 12 de diciembre de 2019, disponible: https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25.
[93] Joseph Solís, "¿Cómo ocurrieron los ciberataques a la banca en Chile y México?, *COBIS*, en línea, consulta: 29 de septiembre de 2019, disponible: http://blog.cobiscorp.com/ciberataques-banca-chile-mexico.
[94] Ibid.
[95] "¿Qué es el ransomware?", *Kaspersky Lab*, en línea, consulta: 30 de septiembre de 2019, disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware.

este tipo de software, Chile se encuentra en el puesto 10°, concentrando un 1.8% del total global.[96] Sin lugar a dudas, esta información resulta muy alarmante, sobre todo si consideramos que, según información entregada por NovaRed, empresa especialista en ciberseguridad, los ciberataques aumentaron en un 59% en Chile entre 2017 y 2018. Asimismo, según Kaspersky Lab, en Latinoamérica se incrementaron en un 60% los ataques cibernéticos en 2018, llegando a un promedio de nueve ataques por segundo.[97]

2. Ley 19.223

En el año 1993, se promulgó en Chile la ley 19.223, la cual tipificó por primera vez figuras penales relativas a la informática. Mediante este cuerpo legal se crearon los primeros delitos relativos al ciberespacio en nuestro país, los cuales centraban su atención en la protección de los diferentes sistemas de tratamiento de información.[98] En ese sentido, y en tan solo cuatro artículos, la ley sanciona el acceso —con ánimo de apropiación, uso o conocimiento— a información contenida en redes informáticas y el daño de los sistemas de tratamiento de información, así como el daño y divulgación de los datos contenidos en dichos sistemas.[99]

La ley 19.223 inició su tramitación el 16 de julio de 1991, mediante la moción parlamentaria del diputado José Antonio Viera-Gallo.[100] Ya en dicho proyecto se daba cuenta de que "*son muchos los abusos que, recurriendo a los avances de la ciencia de la información, pueden cometerse. No cuesta gran esfuerzo imaginar el daño que puede causarse a enormes cantidades de personas, si la información contenida en un banco de datos, por ejemplo, el de una AFP, fuera distorsionada, adulterada o destruida por la acción de un operador malintencionado o que busque algún tipo de enriquecimiento ilícito para sí o para terceros*".[101] Por lo tanto, la finalidad de la nueva ley era, precisamente, "*proteger este nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la*

[96] Vicente Pérez Díaz, "Chile fue el décimo país con más ciberataques en 2018", *Pauta*, 18 de marzo de 2019, en línea, consulta: 1 de octubre de 2019, disponible: https://www.pauta.cl/ciencia-y-tecnologia/chile-fue-el-decimo-pais-con-mas-ciberataques-en-2018.
[97] Ibid.
[98] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.*
[99] Ibid.
[100] Historia de la Ley N° 19.223, *Biblioteca del Congreso Nacional de Chile*, 1991, en línea, consulta: 2 de octubre de 2019, disponible: https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/7025/.
[101] Ibid.

calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan. Aquella, por el actual desarrollo tecnológico de la sociedad, merece ser protegida mediante la creación de figuras delictuales nuevas, que pongan de relieve su importancia".[102]

Luego de completar todos los trámites legislativos correspondientes, la ley 19.223 fue publicada en el Diario Oficial el 7 de junio de 1993, entrando así en vigor para todo el territorio nacional. Pese al indiscutido avance que lo anterior significó en términos objetivos para la protección de la información digital en Chile, dicha regulación se basaba en el progreso cibernético de la época, en un tiempo en que Internet en nuestro país era un fenómeno incipiente y de escaso acceso para la ciudadanía.[103] Pese al fuerte desarrollo que ha experimentado la tecnología a nivel global en los últimos treinta años, nuestro marco legislativo actual en materia de ciberdelitos no ha sido modificado ni actualizado desde su fecha de dictación. En ese mismo sentido, cabe destacar que las herramientas de persecución penal en esta materia datan del año 2000, fecha de dictación del Código Procesal Penal, las cuales se han vuelto insuficientes para una adecuada investigación de este tipo de ilícitos, que permita resguardar los derechos de todos los intervinientes en el respectivo procedimiento.[104]

Así, los alcances logrados en su momento por la ley 19.223 se han vuelto obsoletos con el avance de las nuevas tecnologías, tanto por la creación de nuevas formas de ciberdelincuencia como también por la gran cantidad de vacíos legales que la normativa demostró tener con el paso del tiempo.[105] Los inconvenientes generados por dichos vacíos fueron acentuándose a medida que los medios de ejecución de este tipo de delitos se fueron sofisticando, en circunstancias que, como establecimos anteriormente, nuestra regulación no ha sido modificada desde su promulgación.

Actualmente, la conclusión es unánime: se requiere una actualización del catálogo de delitos

[102] Ibid.
[103] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.*
[104] Ibid.
[105] Ibid.

informáticos, teniendo a la vista la evolución de las tecnologías de la información y la comunicación. A través de las nuevas iniciativas legislativas, se busca dar un trato más comprensivo del contexto en que este tipo de ilícitos son cometidos, pues las actuales carencias no solo están dadas por la falta de una tipificación moderna y eficaz, sino también por la falta de medios suficientes para desarrollar las investigaciones penales relativas a delitos informáticos.[106]

3. Contexto nacional actual en materia de ciberseguridad

Todas las circunstancias anteriormente descritas han provocado una paulatina reacción por parte de las autoridades de nuestro país, las cuales en los últimos años han impulsado una serie de medidas tendientes a mejorar la seguridad cibernética y, de esta forma, poder ajustar nuestras políticas a los estándares internacionales que rigen la materia en la actualidad. Dentro de dichas medidas, encontramos, a modo de ejemplo:

a. Marzo de 2015: publicación de las "Bases para una Política Nacional de Ciberseguridad".[107]
b. Abril de 2015: creación del Comité Interministerial sobre Ciberseguridad (CICS), mediante Decreto Supremo N° 533 del Ministerio del Interior y Seguridad Pública.
c. Abril de 2017: publicación de la Política Nacional de Ciberseguridad.
d. Mayo de 2018: nombramiento del primer asesor presidencial en materia de Ciberseguridad.

La actualización de la regulación atingente a los delitos informáticos forma parte de los pilares de la Política Nacional de Ciberseguridad 2017-2022, la cual estipula dentro de sus objetivos principales la "*actualización de nuestra legislación, impulsada por la decisión de adherir a la Convención sobre Ciberdelitos del Consejo de Europa, la mejora y fortalecimiento de la normativa actual y la creación de medidas transversales en lugar de*

[106] Ibid.
[107] "Bases para una Política Nacional de Ciberseguridad", *Ministerio del Interior y Seguridad Pública*, marzo de 2015, en línea, consulta: 8 de octubre de 2019, disponible: https://www.ciberseguridad.gob.cl/media/2015/12/Documento-Bases-Pol%C3%ADtica-Nacional-sobre-Ciberseguridad.pdf.

sectoriales", entre otros.[108]

Es en este contexto en el cual analizaremos de qué manera ha incorporado Chile dicho tratado internacional luego de su ratificación, y cómo ello impacta nuestra legislación actual en materia de ciberseguridad.

3.1 Recepción del Convenio de Budapest en la legislación chilena

En el capítulo anterior, referido a la regulación internacional en materia de ciberseguridad, hicimos alusión al origen y contenido del Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como Convenio de Budapest, el cual constituye el primer tratado internacional sobre delitos cometidos a través de Internet y de otros sistemas informáticos.[109] En el caso de Chile, dicho instrumento fue promulgado el 27 de abril de 2017, mediante el Decreto Ley N° 83 del Ministerio de Relaciones Exteriores, entrando en vigor el 28 de agosto del mismo año, tras su publicación en el Diario Oficial. Ello, luego de su aprobación por el Congreso Nacional, según consta en el Oficio N° 12.986, de 17 de noviembre de 2016, de la Cámara de Diputados. Asimismo, con fecha 20 de abril de 2017, se depositó ante el Secretario General del Consejo de Europa el instrumento de adhesión de la República de Chile al referido tratado.

En ese sentido, el contenido del Convenio de Budapest se volvió vinculante para nuestro país, especialmente respecto a los compromisos internacionales adquiridos con el fin de desarrollar "*una política criminal común frente a la ciberdelincuencia, mediante la homologación de los conceptos fundamentales y del tratamiento de la legislación penal, sustantiva y procesal, así como del establecimiento de un sistema rápido y eficaz de cooperación internacional*".[110] Como ya ha sido establecido, lo anterior se enmarca en un contexto tanto nacional como global en el cual los ataques cibernéticos han generado un alto impacto en diferentes sectores de la economía, razón por la cual urge actualizar nuestro marco

[108] "Política Nacional de Ciberseguridad", *Comité Interministerial sobre Ciberseguridad*, 2017, en línea, consulta: 12 de octubre de 2019, disponible: https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.
[109] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.*
[110] Ibid.

jurídico actual. Por ende, más allá de los referidos compromisos internacionales, existe en la actualidad una problemática en esta materia que debe necesariamente ser abordado como política pública en Chile.

Asimismo, debemos hacer énfasis en que el Convenio de Budapest hace hincapié en que cualquier normativa sobre ciberdelincuencia "*no puede únicamente contener tipos penales, sino que aquéllos deben ser complementados con una normativa procesal que entregue recursos que permitan investigaciones eficaces atendidas las especiales características de la ciberdelincuencia*".[111]

Con todo, cabe mencionar que el propio Decreto Ley N° 83 de 2017 del Ministerio de Relaciones Exteriores fija una serie de declaraciones y reservas que nuestro país establece respecto del alcance y aplicación del Convenio sobre la Ciberdelincuencia en nuestro territorio, referidos principalmente a la exigencia de intencionalidad delictiva y/o ánimo fraudulento para la penalización de ciertas acciones descritas en el tratado, así como la no aplicación de determinados artículos.

3.2 Contenido del proyecto de ley sobre delitos informáticos actualmente en tramitación

En línea con lo anterior, los esfuerzos del Gobierno de Chile para cumplir con sus obligaciones internacionales en este punto han sido centralizados en el proyecto de ley contenido en el boletín N° 12.192-25, el cual fue ingresado al Senado el 25 de octubre de 2018. Dicho proyecto busca establecer normas sobre delitos informáticos que permitan adecuar nuestra legislación a los estándares internacionales, incluyendo mejoras sustantivas y procesales al respecto.

En primer lugar, el contenido sustancial del referido proyecto de ley puede ser resumido en los siguientes puntos[112], los cuales dan cuenta de la forma en que el Estado de Chile está dando cumplimiento a los mandatos contenidos en el Convenio de Budapest (en adelante,

[111] Ibid.
[112] Juan Pablo González, "Proyecto de Ley Delitos Informáticos", *Ministerio del Interior y Seguridad Pública*, noviembre de 2018, en línea, consulta: 3 de octubre de 2019, disponible: http://www.derecho.uchile.cl/dam/jcr:1f0343d2-dc79-4e3d-b8b6-f38a64c0cf9d/leydelitosinformaticos.pdf.

"CB"), en su calidad de instrumento de derecho internacional:

a. Incorpora nuevas definiciones sobre datos informáticos, sistemas informáticos y datos relativos al tráfico (artículo 1 CB).

b. Reformula los tipos penales existentes actualmente en la ley 19.223 y los adecúa a las figuras reconocidas en el Convenio de Budapest, a saber: acceso ilícito (artículo 2 CB), ataques a la integridad de los datos (artículo 4 CB) y del sistema (artículo 5 CB).

c. Incorpora nuevos tipos penales, los cuales se encuentran establecidos expresamente en el Convenio de Budapest:
    - Interceptación o interferencia ilícita de las transmisiones no públicas entre sistemas informáticos, y la captación ilícita de datos transportados mediante emisiones electromagnéticas de sistemas informáticos (artículo 3 CB).
    - Falsificación informática: comprende la introducción maliciosa, alteración, borrado, deterioro, daño, destrucción o supresión que genere datos no auténticos con el propósito que sean tomados o utilizados como "auténticos" (artículo 7 CB).
    - Fraude informático: sanciona a quien defraude a otro con la finalidad de obtener un beneficio económico ilícito para sí o un tercero, utilizando la información contenida en un sistema informático o aprovechándose de la alteración, daño o supresión de documentos electrónicos (artículo 8 CB).
    - Abuso de los dispositivos: sanciona a quienes entregaren u obtuvieren para su utilización, importaren, difundieren o realizaren otra forma de puesta a disposición de uno o más dispositivos o programas computacionales u otros datos similares, creados o adaptados principalmente para la perpetración de los delitos de perturbación al sistema informático, acceso ilícito, interceptación ilícita y daño a los datos informáticos (artículo 6 CB).

d. Incorpora una nueva atenuante especial, la cual permite rebajar la pena hasta en un grado cuando se acredite una eficaz cooperación en el esclarecimiento de los hechos investigados o en la identificación de los responsables, entre otros supuestos.

e. Incorpora tres agravantes de la responsabilidad penal:
    - Utilización de tecnologías de encriptación que tengan por principal finalidad la obstaculización de la justicia.
    - Comisión del delito abusando de una posición privilegiada de garante o custodia de datos contenidos en un sistema informático, en razón del ejercicio de un cargo o función.
    - Alteración o interrupción de servicios de utilidad pública como resultado de delitos informáticos.

f. Modifica la ley 20.393 sobre responsabilidad penal de las personas jurídicas, agregando los delitos informáticos (artículo 12 CB).

En segundo lugar, en cuanto a las mejoras procesales que establece el proyecto de ley, estas hacen referencia a los siguientes aspectos:[113]

a. Legitimación activa: el Ministro del Interior, junto con los delegados presidenciales regionales y provinciales, podrán presentar querellas cuando los delitos informáticos interrumpan el funcionamiento de un servicio de utilidad pública.

b. Técnicas especiales de investigación: cuando existieren fundadas sospechas de la participación de una asociación ilícita o agrupación de personas que cometan algún delito contenido en el proyecto de ley, se permite el uso de agentes encubiertos, informantes, entregas vigiladas y controladas e interceptación de comunicaciones, siempre previa autorización judicial.

c. Comiso: se fija una regla especial respecto de los instrumentos del delito informático, los efectos y demás utilidades que se hubieran originado. En caso de que lo anterior fuese imposible de determinar, se podrá decomisar una suma de dinero equivalente al valor de los bienes mencionados.[114]

[113] Ibid.
[114] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.*

d. Instrucciones generales: aquellos antecedentes investigativos que se encuentren en formato electrónico serán tratados en conformidad a los estándares definidos para su preservación o custodia, de acuerdo a las instrucciones del Fiscal Nacional. Ello, con el fin de evitar su pérdida producto de su fácil destructibilidad.

e. Establece modificaciones al Código Procesal Penal:
    - Se agrega el artículo 218 bis, referido a la preservación provisoria de datos informáticos que se encuentren en manos de los proveedores de acceso a Internet hasta la obtención de autorización judicial (artículos 16 y 17 CB).
    - Se reemplaza el artículo 219, fijando un nuevo procedimiento para la entrega, previa autorización por parte de un juez de garantía, de datos o información acerca de las comunicaciones transmitidas o recibidas por las empresas concesionarias del servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet, así como para estos últimos.[115]
    - Se modifica el artículo 222, el cual obliga a las empresas concesionarias del servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos a cumplir las medidas de investigación señaladas en dicho artículo. Se establece la obligación de retener datos relativos al tráfico en ciertas circunstancias, se define a qué tipo de datos se refiere y se fija la obligación de secreto de esta especie de medidas para los encargados de realizar las respectivas diligencias.[116]

Finalmente, y a modo de comentario general al proyecto de ley recién descrito, podemos señalar que, pese a que se hace referencia a la obligación de Chile de propender al establecimiento de un sistema de cooperación internacional, como parte de los compromisos adquiridos tras la adhesión al Convenio de Budapest, dicho elemento no figura regulado de forma expresa en el texto actualmente en tramitación. Sin perjuicio de lo anterior, podemos

[115] Ibid.
[116] Ibid.

asimismo concluir que sí existen ciertos avances en esta materia al momento de analizar la recepción que el mencionado tratado internacional ha tenido en nuestra legislación, cuestión que será tratada a continuación.

4. Incorporación del principio de cooperación jurídica internacional en la normativa chilena vigente sobre ciberseguridad

Como ya hemos establecido en el presente trabajo, la cooperación entre diferentes jurisdicciones es fundamental cuando nos referimos a delitos que ocurren en el ciberespacio. Así, si los Estados son víctimas de ataques cibernéticos en los cuales no es posible identificar el origen de estos, o bien son usados como puente para atacar otros objetivos, la cooperación internacional resulta de la mayor importancia para amortiguar sus efectos nocivos y trazar sus orígenes.[117] A continuación, corresponde analizar si la legislación chilena incorpora efectivamente el principio de cooperación jurídica internacional en esta materia.

Luego de estudiar los diferentes cuerpos normativos relevantes para la ciberseguridad a nivel nacional, podemos concluir que ninguno de ellos regula de forma expresa la cooperación jurídica internacional como un eje fundamental en la prevención y sanción de delitos ocurridos en el ciberespacio. Lo anterior resulta particularmente evidente tras la lectura de la ley 19.223, nuestra norma actual para los delitos informáticos, la cual no posee ninguna alusión a la cooperación internacional, como tampoco lo hacen las otras normas que de forma inorgánica regulan esta materia en Chile.

Ahora bien, la Política Nacional de Ciberseguridad 2017-2022, aprobada durante el segundo gobierno de la presidenta Michelle Bachelet, sí incluye dentro de sus objetivos el establecimiento de relaciones de cooperación en ciberseguridad con otros Estados, y la activa participación en foros y discusiones internacionales. En dicho documento, se reconoce el carácter global y transfronterizo de esta disciplina, y se reconoce que, aunque "*no existen instrumentos normativos específicos, el ciberespacio está regulado tanto por las leyes nacionales como por la normativa internacional general aplicable, por lo que el desafío*

[117]Bruno Barrera, "Cooperación regional en ciberseguridad", *El Mostrador*, 9 de agosto de 2018, en línea, consulta: 5 de noviembre de 2019, disponible: https://www.elmostrador.cl/noticias/opinion/columnas/2018/08/09/cooperacion-regional-en-ciberseguridad/.

consiste principalmente en identificar e interpretar las normas relevantes del derecho internacional aplicables".[118] Además, se refuerza la importancia de adherir al Convenio de Budapest y de adoptar acuerdos multilaterales y bilaterales que fomenten la cooperación y asistencia mutua en ciberseguridad.

En ese sentido, acorde con los objetivos anteriormente enunciados, se establece que el Ministerio de Relaciones Exteriores deberá potenciar "*la relación con otros países en ciberseguridad, bajo diversas modalidades como la asistencia desde o hacia Chile, el intercambio de información y experiencias, la implementación y profundización de mecanismos de diálogo político en la materia, y el empuje de medidas de transparencia y construcción de confianza en el ciberespacio*".[119] Cumpliendo con dicho mandato, el Estado de Chile ha promovido la suscripción de numerosos acuerdos bilaterales de cooperación internacional en temas de ciberdefensa, denominados Memorándum de Entendimiento (MoU, por sus iniciales en inglés). La finalidad de dichos acuerdos es velar por la seguridad en el ciberespacio, estableciendo modalidades de cooperación concreta, tales como el intercambio de información, experiencia y buenas prácticas en el ámbito de la ciberseguridad, la realización de visitas de estudio, el desarrollo de programas de capacitación, entre otros. A la fecha, nuestro país ha firmado este tipo de acuerdos con Estados de diferentes regiones del mundo, tales como España, Colombia, Reino Unido, Israel, Argentina, entre otros.

A continuación, nos corresponde referirnos nuevamente en este punto al Convenio de Budapest, el cual fue recepcionado por nuestro derecho interno siguiendo los elementos que la jurisprudencia ha establecido para estos efectos, a saber, "*la aprobación legislativa, la promulgación del tratado por decreto del Presidente de la República y la publicación en el Diario Oficial del texto del tratado y del decreto promulgatorio*".[120] En ese sentido, y respecto al valor que tienen en Chile los tratados internacionales en relación con las otras fuentes de derecho interno, la doctrina se encuentra conteste en que estos equivalen, al menos, a una ley.[121] Es en función de esto último que, en tanto el Convenio de Budapest forma parte

[118] "Política Nacional de Ciberseguridad", *Comité Interministerial sobre Ciberseguridad*, 23.
[119] Ibid., 22.
[120] Cecilia Medina, "El derecho internacional de los derechos humanos y el ordenamiento jurídico chileno", *Corporación Nacional de Reparación y Reconciliación*, diciembre de 1992, 38.
[121] Ibid.

de nuestro ordenamiento jurídico, corresponde analizar si el principio de cooperación internacional se encuentra recogido en él.

Precisamente, el capítulo III del referido tratado internacional regula esta materia, estableciendo en su artículo 23 los principios generales de dicha regulación. A continuación, se establecen las directrices relativas a cuestiones como extradición, asistencia mutua, información espontánea, así como también los procedimientos respectivos, especialmente en torno a temáticas como conservación y revelación rápida de datos informáticos, acceso transfronterizo a dicha información, entre otras.

Asimismo, se establece el compromiso de formar parte de una Red 24/7, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas o datos informáticos. A este respecto, cabe mencionar que, no obstante que el Decreto Ley N° 83/2017 del Ministerio de Relaciones Exteriores designa efectivamente a diferentes autoridades públicas para cumplir ciertas funciones que el tratado establece, cabe todavía hacerse la pregunta sobre si el Estado de Chile ha cumplido cabalmente con las obligaciones internacionales adquiridas en materia de cooperación internacional tras su adhesión al Convenio de Budapest, cuestión que será desarrollada en profundidad en el siguiente capítulo del presente trabajo.

CAPÍTULO IV: RESPONSABILIDAD INTERNACIONAL Y EL CUMPLIMIENTO DEL ESTADO CHILENO DE SUS OBLIGACIONES INTERNACIONALES EN MATERIA DE CIBERSEGURIDAD

En el capítulo anterior, estudiamos cómo la legislación chilena ha ido incorporando paulatinamente los mandatos de la normativa internacional en materia de ciberseguridad, particularmente en lo referido a la recepción de las obligaciones contenidas en el Convenio de Budapest. En esta sección, analizaremos si el Estado de Chile ha cumplido cabalmente con su deber de cooperación jurídica internacional en materia de ciberseguridad, y las eventuales consecuencias que podrían surgir en caso de no observar dicha obligación en el largo plazo.

Para ello, haremos en primer lugar una breve reseña del derecho internacional de responsabilidad de los Estados y los desafíos que plantea el ciberespacio a la aplicación de sus reglas. Luego, nos centraremos en el deber que surge para los Estados de actuar con la debida diligencia en la regulación de esta materia, para finalmente evaluar las consecuencias que podrían pesar sobre el Estado chileno en caso de que este adoptase una postura pasiva por mucho tiempo respecto de los estándares impuestos por la Convención de Budapest.

1. Generalidades sobre la responsabilidad internacional de los Estados

Todo sistema de derecho se construye a partir del principio básico de que cuando un sujeto incumple una obligación incurre en responsabilidad. Debido a que los Estados son los principales sujetos de derecho internacional, resulta sumamente importante para el sistema internacional contar con normas que regulen la responsabilidad de estos. Fue bajo esa consigna que en el año 1949, dos años después de su creación, la Comisión de Derecho Internacional de las Naciones Unidas se embarcó en la misión de codificar las reglas de derecho internacional aplicables a la responsabilidad de los Estados.[122] Gracias al trabajo realizado por cinco relatores especiales a lo largo de aproximadamente cinco décadas, en la 53º sesión de la Comisión de Derecho Internacional en el año 2001 fueron aprobados los

[122] James Crawford, *State Responsibility: The General Part*, 1st ed. (Reino Unido: Cambridge University Press, 2014), 35-39.

renombrados *Draft Articles on Responsibility of States for Internationally Wrongful* Acts (en adelante, "proyecto de artículos"), con sus respectivos comentarios.[123] Si bien a la fecha este conjunto de artículos no ha sido objeto de un tratado multilateral, gran parte de sus reglas y principios reflejan normas del derecho consuetudinario internacional.[124]

1.1 *Draft Articles on Responsibility of States for Internationally Wrongful Acts*

El proyecto de artículos sobre responsabilidad internacional de los Estados por la comisión de actos ilícitos se encuentra dividido en cuatro partes. Sin embargo, para efectos del presente trabajo, solamente nos remitiremos a las dos primeras, las cuales tratan, respectivamente, las condiciones generales que son necesarias para que exista responsabilidad por parte de un Estado y las consecuencias legales que surgen para un Estado declarado responsable internacionalmente.[125]

1.1.1 Elementos de la responsabilidad internacional de los Estados

Ya en el primer artículo se sienta el principio rector del referido proyecto, conforme al cual la comisión por parte de un Estado de un acto ilícito internacionalmente conlleva la responsabilidad internacional de ese Estado.[126] En seguida, el artículo segundo establece dos elementos o condiciones que deben cumplirse copulativamente para que un Estado sea declarado responsable internacionalmente por una acción u omisión cometida. Dichos elementos son, en primer lugar, que el acto sea atribuible al Estado, y segundo, que dicho acto constituya un incumplimiento de una obligación internacional del Estado.[127]

Conforme al primer elemento subjetivo, que un acto sea "*atribuible*" a un Estado implica que la conducta de un agente del Estado puede ser considerada como un acto del propio Estado

[123] James Crawford, "Articles on Responsibility of States for Internationally Wrongful Acts", 2012, en línea, consulta: 12 de noviembre de 2019, disponible: http://legal.un.org/avl/ha/rsiwa/rsiwa.html.
[124] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ Report 2007, paras. 49 & 209.
[125] International Law Commission, "Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries", 2001, en línea, consulta: 20 de noviembre de 2019, disponible: http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. (en adelante, "ARSIWA").
[126] Ibid.
[127] Ibid.

para efectos de dar lugar a su responsabilidad.[128] La conducta atribuible puede surgir de una acción u omisión realizada por el órgano o agencia estatal facultada para ejercer potestades estatales soberanas (artículo 4), o bien, de una acción u omisión realizada por un privado o entidad no estatal que de igual manera puede ser atribuible al Estado bajo ciertas hipótesis (artículos 5-11). Por regla general, los Estados siempre serán responsables de las conductas positivas o negativas realizadas por sus órganos, ya sea en el ejercicio de potestades legislativas, ejecutivas, judiciales u otras. Con todo, el análisis de la atribución de una conducta a un Estado debe realizarse conforme a criterios objetivos determinados por el derecho internacional y no por el mero reconocimiento de un vínculo factual de causalidad.[129]

Conforme al segundo elemento objetivo, existe un "*incumplimiento de una obligación internacional*" cuando la conducta de un Estado no se adecúa a la conducta exigida por una obligación que ese Estado ha contraído, independiente de su origen o naturaleza.[130] Es importante precisar aquí que el proyecto de artículos no pretende definir el contenido de las reglas primarias que contienen las obligaciones contraídas por los Estados, ya que ello será definido por la fuente de derecho internacional de la cual emana la obligación de que se trate (por ejemplo, un tratado) y que deberá ser revisada a la luz del caso concreto.[131] Finalmente, cabe destacar nuevamente que el incumplimiento de una obligación puede derivarse de un acto positivo de un Estado que resulta en la infracción de una obligación de no hacer, o bien de una omisión que tiene como consecuencia el incumplimiento de una obligación de hacer.

1.1.2 Consecuencias legales de la responsabilidad internacional de los Estados

Conforme al artículo 28 del proyecto de artículos, una vez acreditada la comisión de actos internacionalmente ilícitos y atribuibles a un Estado, surgen consecuencias legales para este. Ello se debe a que las reglas e instituciones de la responsabilidad estatal tienen por objeto resguardar el imperio del derecho y la mantención del respeto por el cumplimiento de las obligaciones internacionales.[132] Con todo, dado que diversas conductas pueden resultar en

[128] Crawford, *State Responsibility: The General Part*, 113.
[129] ARSIWA, cap. II, para. 4.
[130] Ibid., art. 12.
[131] Crawford, *State Responsibility: The General Part*, 215-217.
[132] ARSIWA, pt. II, GC & art. 28.

daños de mayor o menor gravedad, existen distintos remedios o formas de reparación aplicables según las circunstancias del caso. Estas formas de reparación son la restitución (artículo 35), la compensación (artículo 36) y la satisfacción (artículo 37), las cuales podrán requerirse en forma separada o conjunta según cuáles sean las consecuencias del acto ilícito.[133]

En esa línea, la restitución consiste en retrotraer la situación al *status quo* anterior a la comisión del acto ilícito, siempre y cuando se cumplan dos condiciones. Primero, que ello no resulte materialmente imposible, y segundo, que el beneficio obtenido no sea desproporcionadamente mayor al costo en que tendría que incurrir el Estado responsable para dicha restitución.[134] Por su parte, la compensación consiste básicamente en el pago de una suma equivalente al daño pecuniario sufrido y se contempla para aquellos casos en que la restitución no es procedente o en que esta por sí sola resulta insuficiente.[135] Finalmente, cuando el daño no puede ser reparado mediante la restitución y/o la compensación, existe el remedio de la satisfacción. Los comentarios al proyecto de artículos son enfáticos en señalar que se trata de un remedio excepcional que solamente tiene lugar cuando las otras dos formas de reparación no sirven para enmendar el daño causado.[136] En términos amplios, la satisfacción consiste en cualquier medida que pueda ser adoptada por un Estado declarado internacionalmente responsable, sin constituir una restitución o compensación.[137] Un ejemplo de esta medida consistiría en —tal como lo contempla el párrafo 2 del artículo 37, sin pretender agotar las medidas que pueden ser tomadas al señalar este ejemplo— que el Estado responsable reconozca públicamente su incumplimiento y proceda a expresar aquello hacia el Estado dañado, ya sea a través de una disculpa formal o a través de otra forma similar que cumpla el mismo fin.

Independiente del remedio que sea procedente para reparar el daño causado, es importante destacar que siempre que se cumplan los elementos necesarios para que un Estado incurra en responsabilidad internacional, y exista un procedimiento formal ante un órgano judicial

[133] Ibid., art. 34.
[134] Ibid., art. 35.
[135] Ibid., art. 36.
[136] Ibid., art. 37.
[137] Crawford, *State Responsibility: The General Part*, 528.

internacional que así lo declare, existirán consecuencias jurídicas que pesarán sobre el Estado que ha cometido una conducta internacionalmente ilícita. De este principio se sigue que, cada vez que un Estado contrae obligaciones internacionales, ya sea implícita o explícitamente, debe cumplir cabalmente con dichas obligaciones, *so pena* de ser declarado responsable por su incumplimiento.

1.2 La jurisprudencia de la Corte Internacional de Justicia

La jurisprudencia de la Corte Internacional de Justicia (en adelante, "CIJ") ha sido sumamente relevante para el esclarecimiento de la interpretación del proyecto de artículos y para la aplicación de este en forma de práctica uniforme y generalizada, lo cual ha culminado últimamente en el reconocimiento y la formulación de reglas consuetudinarias de derecho internacional. Si bien no es el único órgano judicial que en la práctica ha recurrido al proyecto de artículos en sus fallos,[138] su carácter de órgano judicial principal de la Organización de Naciones Unidas dota a sus sentencias de una importancia especial dentro del sistema judicial internacional.

Algunos fallos emblemáticos de la CIJ que han sentado precedentes fundamentales en materia de responsabilidad estatal incluyen: el caso de actividades militares y paramilitares en y en contra de Nicaragua de 1986 (Nicaragua v. EE. UU),[139] el caso del Canal de Corfú de 1949 (Reino Unido v. Albania),[140] el caso del genocidio bosnio de 2007 (Bosnia y Herzegovina v. Serbia y Montenegro)[141] y el caso relativo al personal diplomático y consular de los Estados Unidos en Teherán de 1980 (EE. UU v. Irán),[142] entre otros. Si bien, conforme al artículo 38 (1) (d) del Estatuto de la CIJ, estas decisiones judiciales solamente ocupan un rol subsidiario dentro de las fuentes del derecho internacional, es indiscutido que la Corte

[138] El CIADI, la Corte Europea y la Corte Interamericana de Derechos Humanos en incontables fallos también han aplicado las reglas del proyecto de artículos sobre responsabilidad internacional de los Estados.
[139] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgement, ICJ Reports (1986), 14.
[140] *Corfu channel case (United Kingdom v. Albania)*, Judgement, ICJ Reports (1949), 4.
[141] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgement, ICJ Reports (2007), 43.
[142] *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgements, ICJ Reports (1980), 3.

procura mantener cierta consistencia judicial en sus fallos.[143]

Ciertamente existen (y existirán) un sin fin de decisiones de la CIJ que aluden al proyecto de artículos sobre responsabilidad internacional de los Estados. No obstante, lo que cabe destacar es el importante lugar que guarda dicho cuerpo normativo dentro de la práctica de la CIJ y su progresiva transformación en reglas consuetudinarias de derecho internacional aplicables a todos los Estados.

1.3 Desafíos planteados por la ciberseguridad a las reglas de responsabilidad internacional de los Estados

La primera pregunta que surge para el derecho internacional en esta materia cuando nos referimos a la ciberseguridad es: ¿son aplicables las reglas del proyecto de artículos sobre responsabilidad internacional de los Estados a las obligaciones referidas al ciberespacio? Tanto el Manual de Tallin 2.0 de 2017[144] como el informe del Grupo de Expertos Gubernamentales de la ONU sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2015[145] han indicado que sí, pero ello no significa que no se presenten dificultades a la hora de adaptar estas reglas al mundo de la red. En efecto, al momento de aplicar las reglas internacionales de responsabilidad en materia de ciberseguridad, se presentan ciertos obstáculos técnicos y jurídicos, derivados de la naturaleza propia del mundo digital. Por una parte, debido al carácter transfronterizo de los ciberdelitos, se presenta un problema de trazabilidad de los actos cibernéticos, y por otra, la cuestión del anonimato bajo el cual puede actuar quien comete el delito complejiza la atribución de la conducta ilícita.[146]

Tal como nos señala el profesor Segura Serrano, un primer desafío que surge para el derecho de la responsabilidad estatal en materia de ciberseguridad, y que se debe al carácter

[143] James Crawford, *Brownlie's Principles of Public International Law*, 8th ed. (Reino Unido: Oxford University Press, 2012), 37-39.
[144] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber* Operations, 79.
[145] "Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional", Documentos oficiales de la Asamblea General, 70º periodo de sesiones (A/70/174), n.d., 2-20.
[146] Segura, "Ciberseguridad y Derecho Internacional", 291–299.

transfronterizo de los fenómenos que la afectan, es la dificultad que se genera al momento de precisar el acto o conducta ilícita. Al respecto, puede que una forma eficaz de trazar estas conductas sea a través de evidencia proporcionada por los propios Estados infractores. Sin embargo, según ha señalado el Grupo de Expertos redactores del Manual de Tallin 2.0, no existe suficiente práctica estatal ni *opinio iuris* que permita zanjar una regla internacional bajo la cual los Estados estén obligados a entregar públicamente dicha clase de evidencia.[147] Por lo anterior, esta cuestión continúa siendo un desafío importante cuando de perseguir la responsabilidad estatal por actos cometidos en el ciberespacio se trata.

Un segundo desafío, también destacado por el profesor Segura Serrano, guarda relación con los estándares aplicables a las reglas de atribución de responsabilidad en materia de ciberseguridad. La discusión sobre cuál es el "*test*" adecuado para determinar si un acto realizado por una entidad no-estatal es o no atribuible a un Estado es un desafío que ha generado gran discusión dentro de la doctrina. Mientras que en el Manual de Tallin 2.0 el Grupo de Expertos pareciera inclinarse por la aplicación del "*effective control test*"[148] —práctica judicial seguida por la CIJ en el caso sobre actividades militares y paramilitares en y en contra de Nicaragua y luego confirmada en el caso del genocidio bosnio[149]—, existe otro sector de la doctrina que cuestiona si es este realmente el estándar más adecuado, teniendo en consideración ciertas particularidades de las ciberoperaciones.[150]

En suma, si bien en la actualidad no existen dudas sobre la aplicabilidad de las reglas del proyecto de artículos sobre responsabilidad internacional de los Estados en materias de ciberseguridad, no se encuentra completamente zanjada la forma en que deben aplicarse estas reglas. Ello, considerando especialmente ciertas particularidades que caracterizan a las conductas cibernéticas y que las diferencian en definitiva de las conductas para las cuales fueron originalmente pensadas las reglas de responsabilidad internacional de los Estados.

---

[147] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 83.
[148] Ibid., 96.
[149] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgement, ICJ Reports (1986), para. 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgement, ICJ Reports (2007), 43, para. 399.
[150] Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", *SSRN Scholarly Paper* (Rochester, NY: Social Science Research Network, 2015), en línea, consulta: 13 de noviembre de 2019, disponible: https://papers.ssrn.com/abstract=2557517.

2. Obligaciones de *due diligence* a las que pueden estar sujetos los Estados

Como establecimos anteriormente, la atribución de responsabilidad internacional tiene como requisitos, en primer lugar, que exista una conducta atribuible a un Estado bajo el derecho internacional, y, en segundo lugar, que dicha conducta constituya el incumplimiento de una obligación internacional del mismo Estado. Sobre el primero de estos elementos, el artículo 2 de los *Draft Articles on Responsibility of States for Internationally Wrongful Acts* establece expresamente que la conducta en cuestión puede tratarse tanto de una acción como de una omisión, siendo este último elemento al cual nos referiremos en detalle a continuación.

2.1 Concepto de *due diligence*

Cuando nos referimos a responsabilidad internacional de los Estados por omisión, el concepto que surge inmediatamente es el de *due diligence*. Al respecto, podemos afirmar de manera preliminar que la obligación que tienen los Estados de no causar daños significativos a otros se reconoce bajo el nombre de *due diligence*, siendo considerado en la actualidad un principio general de derecho internacional.[151]

El desarrollo de este término en el derecho internacional encuentra su origen en los principios generales de "Do-No-Harm", en los cuales se reconoce a dicho concepto como un componente importante a la hora de prevenir el daño entre diferentes Estados.[152] Lo anterior se explica bajo el supuesto de que el *due diligence* constituye la materialización del principio de igualdad de soberanía de los Estados, en tanto establece que estos poseen plena jurisdicción para controlar los asuntos que tienen lugar dentro de sus fronteras, procurando siempre respetar la integridad territorial y política del resto de la comunidad internacional.[153]

De esta forma, para efectos del presente trabajo, nos referiremos al *due diligence* como aquel principio según el cual los Estados están obligados a no permitir a sabiendas que su territorio sea usado para actos contrarios a los derechos de otros Estados, como consecuencia del

[151] Timo Koivurova, "Due diligence", *OPIL*, febrero de 2010, en línea, consulta: 21 de noviembre de 2019, disponible en: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1034.
[152] Akiko Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", *Laws* 7, no. 4 (2018), 2.
[153] Ian Yuying Liu, "State Responsibility and Cyberattacks. Defining Due Diligence Obligations", *Indon. J. Int'l & Comp. L.* 4 (2017), 199.

respeto recíproco que deriva de la propia soberanía.[154] En consecuencia, podemos establecer que el principio de *due diligence* es una obligación legal que se infringe por omisión, en la medida en que no se haya hecho todo lo que se podía hacer para prevenir un daño a otro Estado. A este respecto, "*la omisión no solo implica inacción, sino también el haber tomado medidas inefectivas o insuficientes cuando otras más apropiadas eran factibles, esto es, razonablemente disponibles y practicables*".[155]

A nivel jurisprudencial, la Corte Internacional de Justicia confirmó ya en el año 1949 la naturaleza de este principio como derecho consuetudinario[156] en el caso del Canal de Corfú,[157] en el cual el máximo tribunal internacional sostuvo que era argumento suficiente para declarar la responsabilidad de Albania que esta supo, o *debió haber sabido*, de la presencia de minas en sus aguas territoriales y no hizo nada para advertir a terceros Estados de dicha situación.[158] A mayor abundamiento, en el caso relativo al personal diplomático y consular de los Estados Unidos en Teherán, la misma Corte concluyó que la responsabilidad de la República Islámica de Irán venía dada por la inacción de sus autoridades, las cuales fallaron en tomar las medidas apropiadas, en circunstancias que dichas medidas eran evidentemente requeridas.[159]

Así, podemos ver cómo este concepto ha sido reconocido, tanto a nivel normativo como jurisprudencial, en diferentes ámbitos del ordenamiento jurídico internacional, tales como el derecho ambiental, el derecho del mar, y, en el último tiempo, el derecho del ciberespacio.

2.2 Naturaleza de las obligaciones de *due diligence*

Siguiendo la clasificación clásica de las obligaciones, cabe hacerse la importante pregunta sobre si, en el caso del *due diligence*, nos encontramos frente a obligaciones de medios o de resultado, lo cual resultará de particular relevancia al momento de analizar las condiciones

[154] Ibid., 199.
[155] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 43.
[156] Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", 2.
[157] *Corfu Channel*, ICJ Judgment, 1949.
[158] Ibid.
[159] *US Diplomatic and Consular Staff in Tehran*, ICJ Judgment, 1980.

para dar lugar a responsabilidad internacional. Al respecto, la doctrina ha establecido que en esta materia nos encontramos frente a obligaciones de medio, en las cuales los Estados tienen la obligación de tomar todas las precauciones que se encuentren a su alcance para evitar la ocurrencia de ciberataques que causen daño a otros Estados, sin por ello tener que garantizar que dichos ataques no ocurrirán.[160] En ese sentido, el análisis del incumplimiento de dichas obligaciones debe tomar en consideración si el Estado en cuestión adoptó todas las medidas que eran apropiadas para proteger del ataque al otro Estado, dadas sus circunstancias particulares. Por ende, las obligaciones de *due diligence* no pueden clasificarse como obligaciones de resultado, en tanto la imposición de un deber absoluto de prevenir la comisión de ciberdelitos significaría una carga demasiado gravosa para los Estados, en la medida en que ni aun el país más diligente podría garantizar una red de seguridad cibernética impenetrable.[161]

Lo anterior se encuentra nuevamente recogido en los *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, los cuales establecen que las obligaciones de prevención, dentro de las cuales podemos considerar las de *due diligence*, son usualmente construidas como "obligaciones de mejores esfuerzos". Por ende, se requiere que los Estados adopten todas las medidas razonables y necesarias para prevenir la ocurrencia de un determinado evento, pero sin garantizar que dicho evento no ocurrirá.[162]

2.3 Obligaciones internacionales de *due diligence* en materia de ciberseguridad

En el segundo capítulo del presente trabajo nos referimos a los principales instrumentos internacionales que regulan el ciberespacio, dentro de los cuales mencionamos, entre otros, el Convenio de Budapest y el Manual de Tallin 2.0. En esta sección, nos corresponde analizar cuáles son las obligaciones de *due diligence* que estos imponen y si acaso su incumplimiento puede acarrear responsabilidad internacional para los Estados.

[160] Liu, "State Responsibility and Cyberattacks. Defining Due Diligence Obligations", 201.
[161] Ibid., 202.
[162] ARSIWA, art. 12, commentary.

2.3.1 Ciberdiligencia

En primer lugar, podemos afirmar que los Estados tienen el deber general de prevenir ciberataques que se originan dentro de sus fronteras.[163] Sin embargo, como ya hemos dicho, el estándar de diligencia sobre el cual se va a evaluar la conducta de un Estado deberá basarse en un análisis casuístico que contemple las circunstancias particulares de cada eventual incumplimiento. Ello, por cuanto las herramientas legales y técnicas de cada país varían enormemente, razón por la cual resulta evidente que no se le puede exigir lo mismo a todos los Estados en materia de ciberseguridad.

Dicho eso, cabe preguntarse qué exigencias le plantea el principio de *due diligence* a los Estados en cuanto a su institucionalidad e infraestructura cibernéticas.[164] Esta cuestión es de suma relevancia dadas las características particulares del ciberespacio, en donde un acto internacionalmente ilícito puede tratarse tanto del incumplimiento de normativa aplicable durante tiempos de paz como de aquella aplicable en un conflicto armado.[165] Por ende, es pertinente cuestionarse a qué está obligado un Estado cuando hablamos de ciberdiligencia, ya sea en términos conductuales (acciones u omisiones) como respecto al contexto en el cual esta se desarrolla.

Los últimos avances en materia doctrinal sobre este punto fueron recogidos en el Manual de Tallin 2.0, el cual precisamente reconoce en su Regla N.º 6 la validez del principio de *due diligence* como lineamiento general de la ciberseguridad. Dicha norma establece, en concordancia con el concepto anteriormente establecido, que un Estado debe actuar con ciberdiligencia al no permitir que su territorio, o la infraestructura bajo su control, sea usado para ciberoperaciones que afecten los derechos de otros Estados o produzcan serias consecuencias adversas para estos.[166] Así, se establece un determinado estándar de conducta en materia de ciberseguridad, en virtud del cual se exige que el Estado tome todas las medidas que estén a su alcance para poner término a ciberoperaciones que afecten derechos de, o

[163] Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", 7.
[164] Ibid.
[165] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 85.
[166] Ibid., 30.

produzcan serias consecuencias adversas para, otros Estados.[167]

2.3.2 Responsabilidad internacional por incumplimiento de obligaciones de *due diligence* en materia de ciberseguridad

Ya hemos señalado en reiteradas ocasiones que la responsabilidad internacional puede derivarse de una acción o de una omisión, siempre y cuando esta constituya el incumplimiento de una obligación internacional asumida por un Estado. Sin embargo, en el caso del ciberespacio, dichas obligaciones son escasas. Actualmente, el único instrumento internacional vinculante en materia de crímenes cometidos en Internet es el Convenio de Budapest, dentro del cual podemos identificar obligaciones de *due diligence* que deben ser cumplidas por los Estados signatarios de dicho tratado.

En este sentido, y en lo referido a la cooperación internacional, el artículo 23 del Convenio establece que las partes cooperarán entre sí *en la mayor medida de lo posible*, frase que se repite a lo largo de las siguientes disposiciones en lo relativo a la ayuda mutua, la asistencia en relación a diligencias investigativas, entre otras materias. Esta formulación normativa es propia de obligaciones de *due diligence*, de lo cual podemos concluir que, si dos Estados son parte del Convenio de Budapest e infringen las obligaciones anteriormente mencionadas, se daría lugar a responsabilidad internacional, cuestión que deberá ser resuelta según las reglas de solución de controversias que establece el propio Convenio. Este análisis se centrará, en último término, en si el Estado incumplidor "debió haber hecho más de lo que efectivamente hizo", utilizando para ello un estándar de responsabilidad subjetiva para evaluar la conducta de dicho país.

No obstante, ¿qué ocurre si los Estados no forman parte de dicho tratado? En ese caso, las partes deberán fundar sus pretensiones en el derecho internacional general,[168] que reconoce la validez del *due diligence* como principio general. A falta de obligaciones primarias específicas que permitan declarar un incumplimiento que dé lugar a responsabilidad internacional, la doctrina ha establecido que deben aplicarse los *Draft Articles on*

[167] Ibid., 43.
[168] Jovan Kurbalija, "State responsibility in digital space", *Revista Suiza de Derecho Internacional y Derecho Europeo*, Vol. 26, N° 2, 2016, 11.

Responsibility of States for Internationally Wrongful Acts.[169] Sin embargo, dados los desafíos que se siguen de las características particulares del ciberespacio para el derecho de la responsabilidad de los Estados, resultaría muy restrictivo atribuir responsabilidad a un Estado por actos de un ente no-estatal solo si se prueba la existencia de un control efectivo por parte del Estado, tal como lo exige la regla del artículo 8 del proyecto de artículos. Es por ello que "*se aplica el criterio de la diligencia debida en el marco de la obligación consuetudinaria de no permitir el uso del territorio de un Estado para causar daños en otro Estado (asunto de Canal de Corfú), recogida en el mencionado informe de 2015 y en el Manual de Tallin"*.[170] Así, se evitaría la necesidad de identificar de forma precisa al autor del ciberdelito, de modo de facilitar el cumplimiento del requisito de atribución al Estado.[171]

Es así como llegamos nuevamente al Manual de Tallin 2.0, el cual establece en su Regla N.º 14 que, en materia de ciberseguridad, el derecho internacional impone deberes sobre los Estados que requieren acciones positivas de su parte.[172] Por ende, el fracaso en el cumplimiento de dicho deber se configura como una omisión,[173] la que, para efectos del análisis de responsabilidad internacional, califica como un incumplimiento de las obligaciones de *due diligence* que existen en esta materia.

Para ilustrar el punto anterior, el propio Manual da un ejemplo: "*un Estado que permanece inactivo mientras infraestructura cibernética en su territorio está siendo usada por un grupo terrorista para emprender una ciber operación contra otro Estado se encuentra en violación de esta regla, así también como si un Estado, ante la creíble notificación por parte de otro Estado de que tal actividad está siendo ejecutada, falla al no agotar todas las posibles medidas para ponerle fin*".[174] Así, el incumplimiento del principio de *due diligence* en materia de ciberseguridad puede ocurrir en dos hipótesis: primero, por incumplimiento del deber general de prevenir la comisión de ciberdelitos dentro de la jurisdicción de un Estado, y segundo, por infracción del deber de ejecutar todas las acciones que sean necesarias para

[169] Constantine Antonopoulos, "State responsibility in cyberspace", en *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias y Russell Buchan (Edward Elgar Publishing, 2015), 60.
[170] Segura, "Ciberseguridad y derecho internacional", 293.
[171] Ibid.
[172] Ibid.
[173] Ibid.
[174] International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 43.

evitar la comisión de un acto ilícito, cuando un Estado entra en conocimiento del peligro de que ocurra una actividad ilícita.

3. Evaluación del cumplimiento por parte del Estado chileno del deber de ciberdiligencia y posibles consecuencias jurídicas en el largo plazo

Una vez establecido en qué consiste la obligación de ciberdiligencia y las consecuencias que pueden seguirse para un Estado en caso de incumplir con sus obligaciones internacionales, corresponde analizar si Chile ha cumplido eficazmente con su deber de ciberdiligencia y si, en caso de no ser así, el Estado chileno podría verse enfrentado a posibles consecuencias jurídicas al no contar, en el largo plazo, con un marco normativo que se ajuste al principio de cooperación jurídica en materia de ciberseguridad.

3.1 Análisis del cumplimiento del Estado chileno del deber de contar con un marco normativo e institucional ajustado a los estándares del Convenio de Budapest

Desde el momento en que el Convenio de Budapest entró en vigor en 2017, surgió para Chile la obligación de adoptar las medidas legislativas necesarias para hacer cumplir los mandatos de dicho tratado a nivel doméstico. En otras palabras, mediante la adopción del Convenio de Budapest, nació para Chile un verdadero deber de ciberdiligencia, consistente en el establecimiento de un marco normativo interno ajustado a los estándares internacionales de conformidad con el principio de cooperación jurídica internacional.[175] La pregunta que surge aquí es la siguiente: ¿ha tomado el Estado de Chile las medidas suficientes para cumplir efectivamente con esta obligación?

Como se expresó anteriormente, las obligaciones de *due diligence* son obligaciones de medios y no de resultado. Es por ello que, para determinar si Chile ha cumplido eficazmente o no con su deber de ciberdiligencia, es necesario evaluar si las medidas que han sido adoptadas por el Estado resultan suficientes para cumplir con la obligación primaria.[176] Para que los Estados logren dar cumplimiento a esta obligación, el Convenio de Budapest exige

[175] Consejo de Europa, "Informe Explicativo del Convenio sobre la ciberdelincuencia", 6.
[176] ARSIWA, art. 3, para. 7.

que estos armonicen la regulación de los delitos informáticos en su ordenamiento jurídico interno con aquella establecida por el Convenio, y, además, que cuenten con una institucionalidad interna que permita la investigación y persecución eficaz de dichos delitos y que facilite la cooperación interestatal.[177]

A modo de recuento, los esfuerzos más notorios del Estado de Chile para ajustar su regulación y fiscalización interna en materia de ciberseguridad a los estándares internacionales son los siguientes:

a. Promulgación de la ley 19.223, la cual tipificó por primera vez figuras penales relativas a la informática en el año 1993.[178]
b. Creación de la Brigada Investigadora del Cibercrimen (BRICIB) de la PDI en el año 2000.[179]
c. Suscripción de acuerdos bilaterales de cooperación internacional en temas de ciberseguridad, denominados Memorándum de Entendimiento (MoU).
d. Creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) en el año 2015, que pasó a establecerse como un departamento de la Subsecretaría del Interior en el 2018.[180]
e. Tramitación del proyecto de ley sobre delitos informáticos, ingresado al Senado en el año 2018.[181]

En primer lugar, en cuanto a la armonización de la regulación de los ciberdelitos en el nivel interno con las figuras penales contempladas en el Convenio de Budapest, es evidente que la normativa vigente que tipifica los delitos informáticos en Chile (Ley 19.223) no se ajusta a las exigencias establecidas por el tratado. No obstante, para hacerse cargo de lo anterior, actualmente se encuentra en tramitación en el Congreso el proyecto de ley que deroga dicha norma y modifica otros cuerpos legales, con el objeto de adecuar la tipificación de los delitos

[177] Consejo de Europa, "Convenio sobre la Ciberdelincuencia".
[178] Ministerio de Justicia, "Ley Nº 19.223", *Ley Chile - Biblioteca del Congreso Nacional*, 7 de junio 1993, en línea, consulta: 11 de diciembre de 2019, disponible: https://www.leychile.cl/Navegar?idNorma=30590.
[179] Policía de Investigaciones, "Cibercrimen," n.d., en línea, consulta: 10 de diciembre de 2019, disponible: https://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen.
[180] "CSIRT", n.d., en línea, consulta: 11 de diciembre de 2019, disponible: https://www.csirt.gob.cl/.
[181] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.*

informáticos a lo dispuesto en el Convenio de Budapest. Tal como se mencionó en capítulos anteriores, debido a que el Convenio contempla normas que por sí solas no son suficientemente completas como para ser aplicadas internamente, se requiere la dictación de medidas legislativas o reglamentarias que las desarrollen a nivel interno,[182] lo cual es precisamente el objetivo del proyecto de ley, según consta en su mensaje.[183]

Teniendo en consideración que el Convenio de Budapest entró en vigor para el Estado chileno en agosto de 2017, y que el proyecto de ley fue ingresado a tramitación por el Congreso en marzo de 2018, podemos concluir, al menos inicialmente, que Chile se encuentra llano a cumplir con las obligaciones impuestas por el Convenio de Budapest en materia legislativa. Con todo, mientras dicho proyecto de ley siga siendo *proyecto* y no *ley*, la iniciativa del Estado de Chile no tiene poder vinculante y, en consecuencia, no altera el estado actual de la regulación en torno a la ciberseguridad. En consecuencia, si bien en la actualidad Chile ha actuado con la debida diligencia al hacer esfuerzos legislativos para ajustar su normativa penal interna a los estándares internacionales, si la legislación vigente llegara a permanecer por mucho tiempo inalterada, el Estado chileno estaría incumpliendo con sus deberes de cooperación internacional jurídica bajo el Convenio de Budapest. En otras palabras, la inactividad o pasividad prolongada del Estado chileno en torno a actualizar su marco regulatorio de ciberseguridad podría, a largo plazo, considerarse como un incumplimiento de obligaciones internacionales exigibles.

Adicionalmente, cabe destacar que, entre los años 2018 y 2019, Chile ha suscrito seis acuerdos de entendimiento con los Estados de Israel, España, Argentina, Colombia, Ecuador y con la OEA.[184] Sin embargo, si bien estos acuerdos han significado un avance muy importante en la incorporación del principio de cooperación internacional en materia de ciberseguridad a nivel interno, y por ende, un actuar diligente por parte del Estado chileno, resulta insuficiente contar con tan solo seis memorándums de entendimiento sobre cooperación en materia de ciberseguridad, dada la cantidad de países con los cuales el Estado chileno mantiene relaciones internacionales. En el largo plazo – bajo el estándar de debida

[182] Benadava, "Las relaciones entre derecho internacional y derecho interno ante los tribunales chilenos", 42.
[183] *Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest*.
[184] Disponibles en: https://www.csirt.gob.cl.

diligencia en el cumplimiento de su obligación de cooperación jurídica internacional en materia de ciberseguridad – es esperable que Chile continúe aumentando la cantidad de acuerdos suscritos con distintos países y organizaciones mundiales.

En segundo lugar, en cuanto al deber de contar con una institucionalidad fiscalizadora eficaz a nivel interno que facilite la cooperación interestatal, la creación de la Brigada Investigadora del Cibercrimen de la PDI (BRICIB) al inicio del nuevo milenio significó un gran avance para Chile en esta materia, especialmente considerando que fue el primer organismo especializado en la persecución de ciberdelitos en el país. La BRICIB nació "*como una respuesta de la PDI al creciente desarrollo de la criminalidad informática en Chile y de la necesidad de contar con unidades dedicadas a la investigación y solución de los problemas que enfrenta la ciudadanía en el mundo virtual globalizado*".[185] Adicionalmente, la BRICIB cuenta con la posibilidad de compartir y comparar experiencias en torno a la persecución de los ciberdelitos con organismos policiales de otros Estados en las Asambleas Generales de la Interpol. Al respecto, cabe destacar que su última versión se desarrolló entre el 15 y el 18 de octubre de 2019 en Santiago de Chile, en la cual fue aprobada la Resolución N.º 3, que transformó al Grupo de Trabajo sobre el Tratamiento de Información (GTI) en un comité permanente de la Asamblea, denominado "Comité sobre el Tratamiento de Datos".[186]

En esta misma línea, debe destacarse el avance que ha significado la creación del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés), el cual, a partir del año 2018, pasó a formar parte de la Subsecretaría del Ministerio del Interior y Seguridad Nacional. Su objetivo estratégico institucional es "*apoyar y fortalecer la acción tecnológica gubernamental, ampliando el uso de tecnologías de información y comunicación en la gestión pública, a través de la mantención y control de la Red de Conectividad del Estado*".[187] La creación del CSIRT responde a la importante necesidad en materia de ciberseguridad de contar con un organismo gubernamental enfocado en dar respuesta a incidentes en seguridad informática. Sin embargo, Chile aún no cuenta con un CSIRT

[185] Policía de Investigaciones, "Cibercrimen".
[186] Interpol, "88th INTERPOL General Assembly", 15 de octubre de 2019, en línea, consulta: 11 de diciembre de. 2019, disponible: https://www.interpol.int/es/Noticias-y-acontecimientos/Eventos/2019/88th-INTERPOL-General-Assembly.
[187] CSIRT, "Quienes somos", n.d., en línea, consulta: 12 de diciembre de 2019, disponible: https://www.csirt.gob.cl/quienes-somos/.

nacional que pueda "*actuar como punto de contacto del país a nivel internacional en materia de seguridad cibernética y coordinar y llevar a cabo actividades de respuesta a incidentes de seguridad informática a nivel nacional*", como lo exige el sistema internacional.[188] Esto último fue refrendado por el director del CSIRT, Carlos Landeros, en el marco de la versión 2019 del Ciclo de Ciberseguridad organizado por la Alianza Chilena de Ciberseguridad, quien recalcó que es de suma importancia para Chile llegar a contar con un CSIRT nacional.[189]

En definitiva, si bien Chile ha avanzado en la dirección correcta en los últimos años al seguir dando cumplimiento a la hoja de ruta establecida por la Política Nacional de Ciberseguridad, aún quedan tareas pendientes para lograr el establecimiento de una institucionalidad interna que logre cumplir íntegramente con el principio de cooperación jurídica internacional. La última versión del Índice Nacional de Ciberseguridad arrojó que, si bien Chile es el país con mayor progreso en conectividad digital de Latinoamérica, esto no se condice con el desarrollo de su ciberseguridad interna.[190] Asimismo, la última versión del Índice Global de Ciberseguridad de 2018 de la Unión Internacional de Telecomunicaciones (UIT), indicó que Chile se sitúa en el lugar N.º 83 a nivel mundial (de 175 Estados miembros) y en el lugar N.º 9 en la región de las Américas, bajando dos puestos en relación al ranking anterior del año 2014, el cual lo situaba en el lugar N.º 7.[191] Además, sumado a estas cifras, expertos en la materia a nivel nacional han destacado la importancia de avanzar hacia un "Sistema Nacional de Ciberseguridad" que cuente con un CSIRT nacional y que defina la infraestructura crítica de información (ICI) del Estado.[192]

---

[188] Organización de los Estados Americanos, "Buenas Prácticas para establecer un CSIRT nacional", abril de 2016, en línea, consulta: 1 de diciembre de 2019, disponible: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

[189] "Director de CSIRT Expone sobre Infraestructuras Críticas", *Ciberseguridad*, 13 de junio de 2019, en línea, consulta: 12 de diciembre de 2019, disponible: /noticias/director-de-csirt-expone-sobre-infraestructuras-criticas/.

[190] NCSI Project Team, "National Cyber Security Index: Ranking", 2019, en línea, consulta: 12 de diciembre de 2019, disponible: https://ncsi.ega.ee/ncsi-index/.

[191] International Telecommunications Union, "Global Cybersecurity Index" (ITU Publications, 2018), en línea, consulta: 3 de diciembre de 2019, disponible: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[192] Diego Bastarrica, "Conocimos el CSIRT: El bunker donde se monitorean los ciberataques al Gobierno" *FayerWayer*, 5 de noviembre de 2019, en línea, consulta: 12 de diciembre de 2019, disponible: https://www.fayerwayer.com/2019/11/csirt-ciberataques-monitoreo-gobierno-estado/.; Kenneth Pugh, "Ciberseguridad: La nueva institucionalidad que Chile necesita", *Cooperativa*, 21 de junio de 2019, en línea,

En suma, si bien Chile en la actualidad ha actuado con la debida diligencia para cumplir con sus deberes internacionales en materia de ciberseguridad en el corto plazo, aún se encuentra al debe en materias esenciales, como lo son la actualización de la normativa vigente sobre delitos informáticos y el establecimiento de una institucionalidad nacional que permita dar cumplimiento íntegro al principio de cooperación internacional.

Al respecto, debemos hacer presente que el artículo 23 del Convenio de Budapest establece que los países cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del propio tratado, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno. En consecuencia, considerando que el Estado de Chile actualmente sí cuenta con normas relativas a la extradición y a la asistencia mutua en materia penal, los principales esfuerzos que le corresponderían realizar para dar pleno y efectivo cumplimiento a las obligaciones contenidas en el Convenio de Budapest dicen relación con dos grandes temas:

a. A nivel **normativo**, es efectivo que el proyecto de ley actualmente en tramitación viene a paliar en gran medida el evidente déficit legal que existe en materia penal y procesal penal en lo relativo a la ciberseguridad en nuestro derecho interno. En ese sentido, en dichos ámbitos no cabría referirse a un vacío legal propiamente tal, sin perjuicio del análisis posterior que se puede realizar respecto a si los tipos penales regulados cumplen o no con los estándares internacionales que debe cumplir Chile.

b. A nivel **institucional**, como ya establecimos, Chile no cuenta actualmente con un sistema nacional organizado que permita reaccionar con la velocidad que se requiere para hacer frente a la ciberdelincuencia. Ese déficit debe necesariamente ser llenado a través de normas de carácter legal que permitan cumplir con las exigencias que el Convenio impone en lo relativo a la formación de una institucionalidad robusta que fortalezca, entre otras cosas, la asistencia informática internacional, la conservación de la información, el acceso a esta por parte de otras jurisdicciones, etc., entre otras

consulta: 12 de diciembre de 2019, disponible: http://opinion.cooperativa.cl/opinion/ciencia-y-tecnologia/ciberseguridad-la-nueva-institucionalidad-que-chile-necesita/2019-06-21/195935.html.

cuestiones no tratadas por el actual proyecto de ley.

A modo de conclusión, podemos afirmar que, si bien Chile actualmente se encuentra llano a cumplir con sus obligaciones internacionales en materia de cooperación jurídica internacional, y a la fecha ha logrado obrar con la debida diligencia, si en el largo plazo no logra actualizar y ajustar el estado actual de la regulación de la ciberseguridad a los estándares internacionales exigibles, su pasividad prolongada podría transformarse en un incumplimiento de deberes de ciberdiligencia.

Finalmente, es necesario destacar que el nivel de diligencia debida por los estándares internacionales a los cuales se encuentra obligado Chile en lo relativo a la cooperación internacional se complejiza constantemente conforme a los diversos cambios que sufre el ciberespacio. En ese sentido, nuestro país debe estar continuamente revisando su marco normativo en esta materia con el fin de elevar los estándares de sus reglas internas, dotándolas de la suficiente flexibilidad que se requiere para hacer frente de forma efectiva a los nuevos desafíos virtuales.

3.2 Consecuencias para Chile de no contar con un marco normativo ajustado al principio de cooperación internacional en materia de ciberseguridad en el largo plazo

En la sección anterior, establecimos que si Chile llegara a adoptar un actuar pasivo prolongado respecto a sus deberes de cooperación jurídica internacional en materia de ciberseguridad, podría llegar a considerarse como un Estado incumplidor de obligaciones internacionales. A continuación, corresponde analizar cuáles podrían ser los efectos que se podrían generar para el Estado chileno en caso de que, producto de una prolongada deficiencia normativa e institucional, se llegara a considerar que ha incumplido con las obligaciones internacionales impuestas por el Convenio de Budapest.

Como establecimos anteriormente, un Estado podría incurrir en responsabilidad internacional cuando falla en su deber de tomar acciones concretas para evitar la comisión de actos ilícitos en el ciberespacio y, más concretamente, en cooperar con otros Estados en su prevención e

investigación.[193] Dichas obligaciones, a las que hemos clasificado como de *due diligence*, se refieren a, por ejemplo, la adopción de una estrategia a nivel nacional contra el cibercrimen, la investigación significativa de estos tipos de delitos, la cooperación con los Estados víctimas de estos ataques en sus propias pesquisas, entre otras.[194]

En ese sentido, – y considerando que el marco regulatorio de ciberseguridad vigente en Chile no se ajusta correctamente a los estándares exigidos por el Convenio de Budapest – en caso de que la situación actual se llegara a prolongar permanentemente en el tiempo, Chile podría llegar a verse expuesto a una eventual demanda por responsabilidad internacional, por no realizar los esfuerzos correspondientes para regular dicha cuestión en lo relativo al ciberespacio. En efecto, a juicio de expertos en la materia, los Estados tienen deberes de *due diligence* en relación con su infraestructura y actividad cibernética, ya sea pública o privada, que ocurra dentro de sus fronteras.[195] Entonces, *"si un Estado no cumple con dichas obligaciones, el Estado víctima puede reclamar el derecho a reparaciones legales cuando sea apropiado*".[196]

Una vez establecido lo anterior, debemos hacernos la siguiente pregunta: ¿sobre quién recae la carga de la prueba en este caso?, ¿sobre el Estado demandante o sobre el Estado demandado? Para resolver esta interrogante, recurriremos a un caso hipotético: ante una eventual acusación por infringir deberes de ciberdiligencia, el Estado X, en calidad de demandado, podría argumentar, en primer lugar, que efectivamente se realizaron los mejores esfuerzos para prevenir la ocurrencia del delito en cuestión, pero que se falló en el intento ante la creación de nuevos métodos de ataque cibernético, hasta ese momento desconocidos. Asimismo, se podría argüir que no se contaba con la capacidad técnica al momento de la comisión del acto ilícito, debido a circunstancias externas que no le son imputables, o bien, que no contaba con los conocimientos suficientes como para hacer frente a este tipo de exigencias. En ese sentido, queda claro que la carga de la prueba pesa sobre el Estado demandante, en tanto este deberá demostrar que las medidas adoptadas por X no fueron

[193] Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", 11.
[194] Kurbalija, "State responsibility in digital space", 16.
[195] Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", 10.
[196] Ibid.

suficientes para evitar el daño causado, considerando el estándar de diligencia debida exigible a partir del caso concreto.[197]

Sin embargo, no debemos olvidar que, para que se genere dicha responsabilidad, la doctrina ha establecido que el ciberataque en cuestión debe producir *perjuicios graves* para otro Estado, los cuales pueden tratarse o bien de daños físicos a individuos u objetos, o bien de la inhabilitación de su red cibernética.[198] En ese sentido, "*un Estado que no ejerció la ciberdiligencia debida sólo es responsable después de la ocurrencia de actos hostiles contrarios a los derechos legales de otro Estado*",[199] no antes. En definitiva, no basta con la mera falta al deber de ciberdiligencia por parte de Chile, sino que debe existir un daño significativo para que se pueda hablar de responsabilidad internacional.

Finalmente, ¿en qué se materializaría una eventual sentencia desfavorable para Chile en materia de ciberdiligencia? En este caso, si se establece efectivamente el incumplimiento de una obligación de *due diligence* en el ciberespacio, los Estados víctimas de dicha negligencia podrían exigir reparaciones,[200] las cuales serán determinadas de forma casuística según la entidad y magnitud del daño causado. Esto último se encuentra regulado en los *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, los cuales se refieren, como ya establecimos, a las diferentes formas que dicha reparación puede adoptar (restitución, compensación y satisfacción). Aplicadas al ciberespacio, estas presentan las siguientes características:[201]

1. Restitución: en el caso de ciberataques, esta solo puede ser usada si es posible y proporcional al perjuicio sufrido.
2. Compensación: se trata de una opción más plausible cuando se trata de daño ocasionado por un ciberataque. El monto dependerá del establecimiento de un nexo causal directo entre el acto ilícito y los perjuicios resultantes.
3. Satisfacción: puede ser usado en casos de ciberseguridad, como una forma de reconocimiento del daño causado.

[197] Liu, "State Responsibility and Cyberattacks. Defining Due Diligence Obligations", 254.
[198] Ibid., 197.
[199] Ibid., 242.
[200] Ibid., 193.
[201] Kurbalija, "State responsibility in digital space", 16.

En conclusión, la gran consecuencia para Chile de no contar en el largo plazo con un marco normativo ajustado al principio de cooperación internacional en materia de ciberseguridad se refiere a que, cumpliéndose con todos los elementos descritos, podría verse en la obligación de reparar un daño generado por su propia negligencia a otro Estado. Al respecto, el medio de reparación más adecuado para enmendar el daño causado dependerá de la clase de perjuicio que se haya ocasionado.[202] Además, se generarían efectos a nivel interno, ya que podría darse el caso de que ciberdelitos cometidos dentro del territorio nacional no puedan ser correctamente investigados y juzgados por no contar con las herramientas necesarias, lo cual dejaría un espacio de impunidad incompatible con un Estado de Derecho.

Ahora bien, no debemos olvidar que esta lógica aplica (convenientemente) también en sentido inverso. Si Chile se viera afectado por un ataque cibernético que tiene su origen en la infracción de un deber de *due diligence* de otro Estado en materia de ciberseguridad, también podría demandar una reparación apropiada (nuevamente, cumpliéndose los requisitos ya detallados en la presente sección).

[202] Ibid.

CONCLUSIÓN

Si hay algo que está claro hoy en día es que vivimos en un mundo cada vez más globalizado e interconectado. Las distancias que antes parecían insalvables hoy se recorren en milésimas de segundos a través de Internet, cuestión que obliga a los países que conforman la comunidad internacional a repensar sus sistemas normativos para hacer frente a los nuevos fenómenos generados por las tecnologías de la información. Es así como a lo largo del presente trabajo hemos podido constatar que el horizonte legislativo en esta materia, tanto a nivel internacional como nacional, se encuentra innegablemente orientado a la cooperación entre las diferentes naciones a la hora de regular exitosamente el espacio digital. Particularmente en lo relativo a la ciberseguridad, "*dado que todos los Estados tienen la obligación de prevenir el daño transfronterizo según el derecho consuetudinario, estos deben garantizar que las actividades dentro de su jurisdicción no causen daño a otros Estados o áreas más allá de su jurisdicción nacional, y la cooperación internacional rápida parece ser la clave para una exitosa prevención de incidentes cibernéticos*".[203]

Para finalizar el presente trabajo, corresponde identificar cuáles fueron los hallazgos más importantes que pudimos identificar a partir de nuestra pregunta de investigación inicial, la cual buscaba responder si se ha incorporado exitosamente en el derecho chileno el principio de cooperación internacional al legislar temas de ciberseguridad. Luego de haber realizado un extenso análisis tanto de la normativa internacional como de la normativa nacional de ciberseguridad, así como del marco de responsabilidad internacional de los Estados en esta materia, nuestras principales conclusiones son las siguientes:

1. **En la actualidad, existen considerables esfuerzos por parte del Estado chileno para incorporar debidamente el principio de cooperación internacional en materia de ciberseguridad. Sin embargo, muchos de ellos aún no se encuentran materializados, por lo que una prolongada pasividad por parte del Estado chileno podría hacerlo incurrir en responsabilidad internacional.**

[203] Takano, "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications", 11.

2. Lo anterior se demuestra, en primer lugar, a nivel legislativo, especialmente considerando que Chile todavía no cuenta con un catálogo de delitos informáticos tipificados ajustados a los estándares internacionales de cooperación jurídica que exige el Convenio de Budapest, dado que el proyecto de ley aún se encuentra en tramitación en el Congreso.

3. También se encuentra evidenciado a nivel institucional, particularmente debido a la ausencia de un Sistema Nacional de Ciberseguridad formado por una institucionalidad que realmente permita la cooperación entre Estados al perseguir delitos cibernéticos. Sin perjuicio de lo anterior, es innegable que han existido importantes avances concretos en este tema a nivel interno, como lo ha sido el establecimiento del CSIRT (cumpliendo con la agenda de la Política Nacional de Ciberseguridad), la suscripción de varios acuerdos bilaterales en temas de ciberdefensa y la clara intención de mejorar la normativa aplicable a los ciberdelitos con el mencionado proyecto de ley.

4. Sin embargo, en el largo plazo estas medidas no se hacen cargo de forma categórica de los lineamientos fundamentales que los propios instrumentos internacionales ratificados por Chile han establecido en esta materia, o bien, resultan insuficientes para hacer frente a las complejidades propias de los delitos cometidos en el espacio digital. Al respecto, debemos recordar que el Convenio de Budapest comienza su preámbulo señalando que el objetivo del tratado es lograr una unión más estrecha entre los Estados signatarios,[204] reconociendo el principio de cooperación internacional como un eje central a la hora de regular asuntos de ciberseguridad a nivel doméstico, lo que finalmente se ve reflejado a lo largo de todas sus disposiciones. Es por ello que resulta fundamental que Chile haga los esfuerzos correspondientes para contar tanto con un marco normativo como con una institucionalidad que permitan una colaboración efectiva con otros Estados a la hora de investigar y perseguir delitos cibernéticos.

[204] Consejo de Europa, “Convenio sobre la Ciberdelincuencia”, 1.

En la actualidad, estos temas pueden todavía resultar desconocidos para la mayoría de la población, lo que trae como consecuencia que su efectiva incorporación desde el derecho internacional a nuestra normativa interna no sea una prioridad a nivel de agenda nacional. En este sentido, el presente trabajo busca enfatizar la importancia de que el Estado de Chile efectivamente llegue a cumplir cabalmente con sus obligaciones internacionales a la hora de regular materias de ciberdelincuencia, siempre teniendo en la mira una correcta recepción del principio de cooperación internacional, so pena de incurrir en responsabilidad internacional por permanecer pasivo respecto al cumplimiento de estas obligaciones por un período muy prolongado de tiempo.

En relación con lo anterior, dicha importancia se ha visto especialmente reforzada por la crisis sanitaria que se encuentra actualmente en desarrollo como consecuencia de la propagación del virus COVID-19. Como medida de contención frente a esta pandemia, gran parte de la población mundial ha tenido que aislarse socialmente, lo que ha traído como resultado que el ciberespacio y los vínculos que se generan a través de él tengan una importancia inédita en nuestra historia. Desde cuestiones cotidianas como reuniones de trabajo hasta sesiones de órganos legislativos y judiciales, en donde la confidencialidad juega un rol absolutamente primordial, tienen lugar hoy a través de las distintas plataformas digitales, lo que hace que las temáticas aquí planteadas cobren especial relevancia.

Finalmente, si bien es verdad que a la fecha no ha existido ningún caso concreto que vulnere gravemente la prohibición al uso de la fuerza en derecho internacional, monitoreos en tiempo real han registrado que en la actualidad ocurren más de seis millones de ciberataques al día, lo cual ha producido una sensación de inseguridad cibernética mundial.[205] Debido a ello, los países se han preocupado de invertir cada vez más en mejorar sus capacidades para defenderse de los ciberataques, iniciando así una suerte de "militarización" del ciberespacio.[206] En ese marco, ante temáticas tan sensibles para la ciudadanía como son la correcta realización de procesos eleccionarios o la seguridad de los fondos bancarios, que debiesen permanecer exentos de intervención externa a través de *hackeos*, el derecho chileno debe anticiparse a la ocurrencia de hechos delictuales que podrían traer gravísimas

[205] Liu, "State Responsibility and Cyberattacks. Defining Due Diligence Obligations", 195.
[206] Ibid.

consecuencias para la población. De esta manera, no queda ninguna duda de que, como señala Antonopoulos, "*el mejor curso de acción para lograr el cese de actos cibernéticos perjudiciales pareciera ser a través de la adopción de buenas prácticas en Internet y [sobre todo] la cooperación internacional*".[207]

[207] Antonopoulos, "State responsibility in cyberspace", 71.

REFERENCIAS BIBLIOGRÁFICAS

Libros y artículos de revistas

1. Antonopoulos, Constantine. "State responsibility in cyberspace". En: *Research Handbook on International Law and Cyberspace*, editado por Nicholas Tsagourias y Russell Buchan. Edward Elgar Publishing, 2015.

2. Beeson, Thomas, y Denning, Dorothy. "Cyberwarfare". *IEEE Security & Privacy* 9, 2011.

3. Benadava, Santiago. "Las relaciones entre derecho internacional y derecho interno ante los tribunales chilenos". En: *Nuevos enfoques del derecho internacional*, coordinado por Avelino León. Santiago, Chile: Editorial Jurídica de Chile, 1992.

4. Brenner, Susan. "La Convención sobre Cibercrimen del Consejo de Europa". *Revista Chilena de Derecho y Tecnología 1*, no. 1, 2012.

5. Carbonnier, Jean. Derecho flexible. Para una sociología no rigurosa del Derecho. Madrid: Ed. Tecnos, 1974.

6. Cerezo, Ana I., Javier López y Ahmed Patel. "International Cooperation to Fight Transnational Cybercrime". *Second international workshop on digital forensics and incident analysis*. WDFIA, 2007.

7. Crawford, James. "Articles on Responsibility of States for Internationally Wrongful Acts", *United Nations Audiovisual Library of International Law*, 2012.

8. Crawford, James. *Brownlie's Principles of Public International Law*, 8th ed. Reino Unido: Oxford University Press, 2012.

9. Crawford, James. *State Responsibility: The General Part*, 1st ed. Reino Unido: Cambridge University Press, 2014.

10. Domingo, Rafael. "¿Por qué un Derecho Global?". En: *Hacia un Derecho Global: Reflexiones en torno al Derecho y la Globalización*, coordinado por Aparicio Caicedo, Rafel Domingo y Martín Santiváñez. Cizur Menor, Navarra: Editorial Aranzadi, 2006.

11. Hedocia, Mauricio. "Los Principios de Derecho Internacional Contenidos en la Carta de la OEA". n.d, en línea, consulta: 29 de agosto de 2019, disponible: https://www.oas.org/dil/esp/XXXVIII_Curso_Derecho_Inter.

12. International Group of Experts at the NATO Cooperative Cyber Defense Centre of Excellence. *Tallinn Manual 2.0 on the International Law Applicable to Cyber*

Operations. Reino Unido: Cambridge University Press, 2017.

13. Kurbalija, Jovan. "State responsibility in digital space", *Revista Suiza de Derecho Internacional y Derecho Europeo,* Vol. 26, N° 2, 2016.

14. Liu, Ian Yuying. "State Responsibility and Cyberattacks. Defining Due Diligence Obligations". *Indon. J. Int'l & Comp. L.* 4, 2017.

15. Llorens, María Pilar. "Los desafíos del uso de la fuerza en el ciberespacio". *Anuario Mexicano de Derecho Internacional* 1, no. 17, 2017.

16. Lorents, Peter, Rain, Ottis y Raul, Rikk. "Cyber Society and Cooperative Cyber Defense". *International Conference on Internationalization, Design and Global Development*. Springer, Berlín y Heidelberg, 2009.

17. Macak, Kubo. "Is the International Law of Cyber Security in Crisis?". *8th International Conference on Cyber Conflict*. Tallinn, 2016.

18. Margulies, Peter. "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility". *SSRN Scholarly Paper*. Rochester, NY: Social Science Research Network, 2015.

19. Medina, Cecilia. "El derecho internacional de los derechos humanos y el ordenamiento jurídico chileno", *Corporación Nacional de Reparación y Reconciliación*, 1992.

20. Morillo, Javier, ed. "La cooperación internacional y el derecho". En: *La cooperación internacional y su régimen jurídico en Colombia.* Bogotá: Agencia Presidencial para la Acción Social y la Cooperación Internacional, 2008.

21. Murat Dogrul, Adil Aslan y Eyyup Celik. "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism". *3rd International Conference on Cyber Conflict*. Tallinn, 2011.

22. OECD. "Digital Security Risk Management for Economic and Social Prosperity". Paris: OECD Publishing, 2015.

23. Pipyros, Kosmas, Lilian Mitrou, Dimitris Gritzalis y Theodorus Apostolopoulos. "Cyberoperations and international humanitarian law". *Information & Computer Security*, 2016.

24. Pons Gamon, Vicente. "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cibercrime, ciberterrorism, legislation and cibersecurity". *URVIO. Revista Latinoamericana de Estudios de Seguridad* 20, 2017.

25. Rayón, María Concepción, y José Antonio Gómez. "Cibercrimen: particularidades en

su investigación y enjuiciamiento". *Anuario Jurídico y Económico Ecurialense* XLVII, 2014.

26. Sancho Hirane, Carolina. "Ciberinteligencia: Contextualización, Aproximación Conceptual, Características y Desafíos". *Cuaderno de trabajo* 1. Santiago: Centro de Investigaciones y Estudios Estratégicos, 2018.

27. Schjolberg, Stein. "The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva". *Journal of International Commercial Law and Technology* 1, no. 12, 2008.

28. Segura, Antonio. "Ciberseguridad y derecho internacional". *Revista Española de Derecho Internacional* 69, no. 2. Madrid, 2017.

29. Takano, Akiko. "Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications". *Laws* 7, no. 4, 2018.

30. Villalta Vizcarra, Ana Elizabeth. "Cooperación jurídica internacional en materia civil y penal". *Rev. secr. Trib. perm. revis.* 5, no. 10, 2017.

Normativa y otros documentos legales

1. Acuerdo sobre Extradición entre el MERCOSUR, La República de Bolivia y la República de Chile, 1998.

2. Bases para una Política Nacional de Ciberseguridad, *Ministerio del Interior y Seguridad Pública*, 2015.

3. Carta de las Naciones Unidas, Organización de las Naciones Unidas, 1945.

4. Carta de la Organización de los Estados Americanos, Organización de los Estados Americanos, 1948.

5. Convención Interamericana sobre Asistencia Mutua en Materia Penal, Organización de Estados Americanos, 1992.

6. Convenio sobre la Ciberdelincuencia, Consejo de Europa, 2001.

7. Declaración de Río sobre el Medio Ambiente y el Desarrollo, Organización de las Naciones Unidas, 1992.

8. Decreto N° 83, Ministerio de Relaciones Exteriores que Promulga el Convenio Sobre la Ciberdelincuencia, 2017.

9. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, International Law Commission, 2001.

10. Estatuto de la Corte Internacional de Justicia, Organización de las Naciones Unidas, 1945.

11. Estatuto de Roma, Corte Penal Internacional, 1998.

12. Historia de la Ley N° 19.223, Biblioteca del Congreso Nacional de Chile, 1991.

13. Política Nacional de Ciberseguridad, *Comité Interministerial sobre Ciberseguridad*, 2017.

14. Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, Documentos oficiales de la Asamblea General, 70º periodo de sesiones (A/70/174).

15. Ley Nº 19.223, Ministerio de Justicia, 1993.

16. Principios Fundamentales del Movimiento de la Cruz Roja y de la Medialuna Roja, Comité Internacional de la Cruz Roja.

17. Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley Nº 19.233 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest, 2018.

18. Reglamento General de Protección de Datos de la UE, Parlamento Europeo y Consejo de la Unión Europea, 2016.

19. Tratado de Extradición entre Chile y Colombia, 1929.

20. Tratado de Extradición entre Chile y el Gobierno de la República de los Estados Unidos de América, 1902.

21. Tratado de Extradición entre Chile y Perú, 1936.

Jurisprudencia

1. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro),* Judgement, ICJ Reports (2007).

2. *Corfu channel case (United Kingdom v. Albania),* Judgement, ICJ Reports (1949).

3. *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United*

States of America), Merits, Judgement, ICJ Reports (1986).

4. *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran),* Judgements, ICJ Reports (1980).

5. Whaling in the Antarctic (Australia v. Japan: New Zealand intervening), Judgement, ICJ Reports (2007).

Sitios web

1. ¿Qué es el ransomware?, *Kaspersky Lab*, en línea, consulta: 30 de septiembre de 2019, disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware.

2. ¿Qué es la cooperación?, *Agcid Chile*, en línea, consulta: 20 de septiembre de 2019, disponible: https://www.agci.cl/que-es-la-cooperacion.

3. Adoption of Convention on Cybercrime", *The American Journal of International Law* 95, no. 4 (2001), pp. 889–891, en línea, consulta: 1 de octubre de 2019, disponible: www.jstor.org/stable/2674643.

4. Arab Regional Cyber Security Center, n.d., en línea, consulta: 24 de octubre de 2019, disponible: https://arcc.om/?GetLang=en.

5. Asociación por los Derechos Civiles, "La Convención de Cibercrimen de Budapest y América Latina: Breve guía acerca de su impacto en los derechos y garantías de las personas", marzo 2018, en línea, consulta: 3 de diciembre de 3019, disponible: https://adcdigital.org.ar/wp-content/uploads/2018/03/Convencion-Budapest-y-America-Latina.pdf.

6. Banco Mundial, "Personas que usan Internet (% de la población) | Data" (n.d.), online, consulta: 25 de septiembre de 2019, disponible: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS.

7. Barrera, Bruno. "Cooperación regional en ciberseguridad", *El Mostrador*, 9 de agosto de 2018, en línea, consulta: 5 de noviembre de 2019, disponible: https://www.elmostrador.cl/noticias/opinion/columnas/2018/08/09/cooperacion-regional-en-ciberseguridad/.

8. Bastarrica, Diego. "Conocimos el CSIRT: El bunker donde se monitorean los ciberataques al Gobierno". *FayerWayer*. 5 de noviembre de 2019. En línea, consulta: 12 de diciembre de 2019, disponible: https://www.fayerwayer.com/2019/11/csirt-ciberataques-monitoreo-gobierno-estado/.

9. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise., n.d., en línea, consulta: 1 de octubre de 2019, disponible: https://ccdcoe.org/.

10. Challenges to effective EU cybersecurity policy, *European Court of Auditors*, marzo 2019, en línea, consulta: 2 de septiembre de 2019, disponible: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf.

11. Christiansen, Axel y Rodríguez, Francisco. "La historia del primer computador que llegó a Chile", *La Tercera*, 17 de septiembre de 2019, en línea, consulta: 23 de septiembre de 2019, disponible: https://www.dcc.uchile.cl/sites/default/files/dcc_prensa/2010/0970_La%20Tercera_El%20primer%20computador.pdf.

12. Comité Jurídico Interamericano CIJ | Misión Permanente de Colombia ante la OEA, n.d., en línea, consulta: 9 de septiembre de 2019, disponible: https://washington-oea.mision.gov.co/comite-juridico-interamericano-cij.

13. Consejo de Europa, "Informe Explicativo del Convenio sobre la ciberdelincuencia", 8 de noviembre de 2001, en línea, consulta: 5 de octubre de 2019, disponible: https://rm.coe.int/16802fa403.

14. CSIRT, "Quienes somos", n.d., en línea, consulta: 12 de diciembre de 2019, disponible: https://www.csirt.gob.cl/quienes-somos/.

15. CSIRT, n.d., en línea, consulta: 11 de diciembre de 2019, disponible: https://www.csirt.gob.cl/.

16. Cybercrime, *Migration and Home Affairs European Commission*, en línea, consulta: 3 de septiembre de 2019, disponible: https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime.

17. Cybercrime, n.d., en línea, consulta: 24 de octubre de 2019, disponible: https://www.interpol.int/en/Crimes/Cybercrime.

18. Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe". *Wired*. 21 de agosto de 2007, en línea, consulta: 16 de septiembre de 2019, disponible: https://www.wired.com/2007/08/ff-estonia/.

19. Director de CSIRT Expone sobre Infraestructuras Críticas, *Ciberseguridad*, 13 de junio de 2019, en línea, consulta: 12 de diciembre de 2019, disponible: /noticias/director-de-csirt-expone-sobre-infraestructuras-criticas/.

20. EUGDPR – Information Portal, n.d., en línea, consulta: 22 de octubre de 2019, disponible: https://eugdpr.org/.

21. González, Juan Pablo. “Proyecto de Ley Delitos Informáticos”, *Ministerio del Interior y Seguridad Pública,* noviembre de 2018, en línea, consulta: 3 de octubre de 2019, disponible: http://www.derecho.uchile.cl/dam/jcr:1f0343d2-dc79-4e3d-b8b6-f38a64c0cf9d/leydelitosinformaticos.pdf.

22. International Telecommunications Union, “Global Cybersecurity Index” (ITU Publications, 2018), en línea, consulta: 3 de diciembre de 2019, disponible: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

23. Interpol, “88th INTERPOL General Assembly”, 15 de octubre de 2019, en línea, consulta: 11 de diciembre de. 2019, disponible: https://www.interpol.int/es/Noticias-y-acontecimientos/Eventos/2019/88th-INTERPOL-General-Assembly.

24. Koivurova, Timo. “Due diligence”, *OPIL*, febrero de 2010, en línea, consulta: 21 de noviembre de 2019, disponible en: https://opil.ouplaw.com/view/101093/law:epil/9780199231690/law-9780199231690-e1034.

25. McGuinness, Damien. “How a cyber-attack transformed Estonia”. *BBC News*. 27 de abril de 2017. Sec. Europe, en línea, consulta: 5 de septiembre de 2019, disponible: https://www.bbc.com/news/39655415.

26. Ministerio de Relaciones Exteriores de Chile - Principios de la Política Exterior Chilena, n.d., en línea, consulta: 9 de septiembre de 2019, disponible: https://minrel.gob.cl/principios-de-la-politica-exterior-chilena/minrel/2008-08-02/194424.html#vtxt_cuerpo_T2.

27. NCSI Project Team, “National Cyber Security Index: Ranking”, 2019, en línea, consulta: 12 de diciembre de 2019, disponible: https://ncsi.ega.ee/ncsi-index/.

28. Organización de los Estados Americanos, “Buenas Prácticas para establecer un CSIRT nacional”, abril de 2016, en línea, consulta: 1 de diciembre de 2019, disponible: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

29. Parties/Observers to the Budapest Convention and Observer Organizations to the T-CY, n.d., en línea, consulta: 30 de septiembre de 2019, disponible: https://www.coe.int/en/web/cybercrime/parties-observers.

30. Pérez Díaz, Vicente. “Chile fue el décimo país con más ciberataques en 2018”, *Pauta*, 18 de marzo de 2019, en línea, consulta: 1 de octubre de 2019, disponible: https://www.pauta.cl/ciencia-y-tecnologia/chile-fue-el-decimo-pais-con-mas-ciberataques-en-2018.

31. Policía de Investigaciones, “Cibercrimen,” n.d., en línea, consulta: 10 de diciembre de 2019, disponible: https://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen.

32. PricewaterhouseCoopers. "¿Cómo afecta a Chile el nuevo Reglamento General de Protección de Datos de la UE?". n.d, en línea, consulta: 10 de octubre de 2019, disponible: https://www.pwc.com/cl/es/prensa/prensa/2018/Como-afecta-a-Chile-el-nuevo-Reglamento-General-de-Proteccion-de-Datos-de-la-UE.html.

33. Pugh, Kenneth. "Ciberseguridad: La nueva institucionalidad que Chile necesita". *Cooperativa*. 21 de junio de 2019, en línea, consulta: 12 de diciembre de 2019, disponible: http://opinion.cooperativa.cl/opinion/ciencia-y-tecnologia/ciberseguridad-la-nueva-institucionalidad-que-chile-necesita/2019-06-21/195935.html.

34. Rees, Albert. "24/7 High Tech Crime Network". 2007, 4n línea, consulta: 10 de diciembre de 2019, disponible: http://www.oas.org/juridico/english/cyb20_network_en.pdf.

35. Solís, Joseph. "¿Cómo ocurrieron los ciberataques a la banca en Chile y México?, *COBIS*, en línea, consulta: 29 de septiembre de 2019, disponible: http://blog.cobiscorp.com/ciberataques-banca-chile-mexico.

36. Statistics, *International Telecommunication Union,* en línea, consulta: 2 de marzo de 2020, disponible: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.