UNIVERSIDAD DE CHILE

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO COMERCIAL.

PROYECTO DE LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN. EVOLUCIÓN DE LA DISCUSIÓN SOBRE ATRIBUCIONES DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD Y LA COMISIÓN PARA EL MERCADO FINANCIERO.

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

AUTOR: JUAN ANTONIO QUEZADA YAÑEZ

PROFESOR GUÍA: CLAUDIO MAGLIONA MARKOVICTH

Santiago de Chile

2023

TABLA DE CONTENIDO

RESUMEN

Este ensayo tiene por finalidad analizar críticamente la evolución de ciertas atribuciones de las que dispondrá la Agencia Nacional de Ciberseguridad que busca ser instaurada por el proyecto de ley N.º 14.847-06 que establece la “Ley marco sobre ciberseguridad e infraestructura crítica de la información”, aquello a la luz de las dificultades que ha evidenciado su discusión parlamentaria puesto que en sus orígenes algunas de aquellas suponían una duplicidad de facultades, concretamente con aquellas que ha desempeñado en materia de ciberseguridad y con cierto grado de experiencia, la Comisión para el Mercado Financiero.

En atención a lo anterior es que este trabajo abarcara una breve, pero necesaria explicación sobre qué entendemos por ciberseguridad y sus aspectos relacionados, la forma en la que nuestro país ha tratado esta temática a lo largo del tiempo, un análisis de la forma en la que se ha propuesto el proyecto de ley y la Agencia Nacional de Ciberseguridad que este crea, así como sus facultades, realizando una comparativa con aquellas que la Comisión para el Mercado Financiero ya posee en la materia, finalizando con el análisis del comportamiento en derecho comparado en torno a la relación que existe entre el agente de ciberseguridad y el regulador financiero como entidad sectorial, todo esto para demostrar que la falta de regulación especial obligó a la entidad financiera nacional a llenar dicho vacío normativo, situación que no ocurre en los países estudiados.

Palabras claves: Ciberseguridad; Agencia Nacional de Ciberseguridad; Comisión para el Mercado Financiero; Prevención de la Duplicidad Normativa.

INTRODUCCIÓN

Con la vertiginosa evolución del internet y las redes de comunicación en el pasado siglo, cambiaría paulatinamente la manera en la que nos desenvolvemos en nuestro diario vivir. Dicha evolución ha supuesto, a día de hoy, que la mayor parte de los individuos tenga acceso a alguna tecnología de la información (TIC), tecnología que a su vez sirve de vehículo para acceder a un entramado digital en el cual se producen múltiples interacciones. En estos días el ejemplo más relevante de esta situación se da con los teléfonos inteligentes y las redes sociales.

Los múltiples servidores y satélites alrededor de nuestro planeta permiten una interconexión global a través del internet, lo cual en principio supuso increíbles beneficios, sobre todo en el aspecto comunicacional, sin embargo, el acceso a la red requiere de un instrumento físico, es decir, una tecnología que permita conectarnos, siendo las más habituales las computadoras o los teléfonos inteligentes. A través de esta tecnología física o material nos volvemos un participante de la red, la cual se canaliza por medio de distintos softwares, los cuales habitualmente requieren de un acceso que incluya un nombre de usuario y una respectiva contraseña para ser utilizados.

Este método de conexión a la red se da en diversos ámbitos de nuestra vida cotidiana, tanto a través de softwares privados como también públicos. Por ejemplo, si queremos acceder a una plataforma de correo electrónico, debemos contar con una dirección de correo y su respectiva contraseña, similares requisitos se pueden exigir para acceder a una plataforma gubernamental donde se ingresa típicamente con el N.º de cédula de identidad y una contraseña.

Pues bien, a pesar de que las redes y el Internet son un entramado de datos de relativa complejidad, desde prácticamente la creación del mismo han existido individuos, externos a su creación, con las capacidades de comprender dicho entramado. Estos individuos han sido mundialmente conocidos como “*hackers*” o piratas informáticos y según la RAE es el término para referirse a una persona con grandes habilidades en el manejo de computadoras, que investiga un sistema informático para avisar de los fallos del mismo y desarrollar técnicas de mejora. Sin embargo, a pesar de que dicha descripción no parece

implicar una amenaza, es necesario esclarecer que un subgrupo de estos sujetos debe su fama por el hecho de utilizar ese conocimiento con fines ilícitos.

En ese contexto, este subgrupo de *hackers* ha supuesto desde los inicios del Internet una amenaza tanto para los ciudadanos como para las instituciones, ya sea público o privadas de los países alrededor de todo el mundo. Es por ello que los entes de seguridad nacional de los diversos Estados se han abocado a crear normativas e instituciones especializadas para paliar las consecuencias que implican la mencionada amenaza.

Lamentablemente, a pesar de los recientes avances en la materia, nuestro país no cuenta en la actualidad con una institucionalidad determinada que se haga cargo de promover la gestión de riesgos y la implementación de estándares de seguridad digital, como es el caso de otros países del mundo. En estas condiciones es que nace el proyecto de ley que establece una "Ley marco sobre ciberseguridad e infraestructura crítica de la información", el cual crea precisamente la llamada Agencia Nacional de Ciberseguridad[1].

Premunida de diversas facultades que analizaremos en el desarrollo del presente trabajo, la referida Agencia se postula como ese ente especializado necesario para proteger la seguridad de las instituciones y las personas en sus interacciones en la red. Sin embargo, esa denominación de ente especializado hizo que, en el proyecto despachado por el Senado, se nos presentara como una institución con amplias facultades en ciberseguridad, suponiendo una duplicidad normativa respecto de las que ya son ejercidas por otra institución como lo es la Comisión para el Mercado Financiero (CMF), situación que inspiró un amplio debate, que requirió de un arduo trabajo de todos los intervinientes.

Justamente en los años recientes, la CMF ha tenido una labor relevante en torno a la ciberseguridad, toda vez que sus regulados son entidades financieras que manejan grandes sumas de dinero, así como también los datos de una gran cantidad de clientes, de tal forma que se han dedicado a establecer lineamientos al respecto y han sido proactivos en divulgar la importancia de la seguridad de las redes.

En este orden de ideas, veremos que el proyecto difiere de la evolución que ha tenido la experiencia comparada en torno a la regulación de la ciberseguridad y por tanto de la relación existente entre el ciber regulador y el regulador financiero, toda vez que en nuestro

[1] CHILE. Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N.º 14.847-06. 2 de marzo de 2022. Disponible en: https://bit.ly/41x2ZEJ

país el desarrollo legislativo fue tardío obligando a la CMF a ejercer facultades para salvaguardar la ciberseguridad respecto de sus regulados. Se aprecia que, en ciertos países, que han resultado ser una inspiración para este proyecto, la creación de un ente especializado se ha decantado por mantener la deferencia del regulador financiero cuando el incidente de ciberseguridad se desarrolla precisamente en el mundo financiero que a él le corresponde regular.

En función de lo anterior, este trabajo abordará en un primer capítulo una necesaria contextualización acerca del internet, el cibercrimen y la ciberseguridad, cómo han sido tratados estos tópicos a rasgos generales con el paso de los años, tanto en una perspectiva internacional como también la evolución que ha habido en nuestro país.

Un segundo capítulo se dedicará a examinar algunos rasgos generales del proyecto de ley en actual discusión parlamentaria, pasando por sus orígenes, y su estructura, con el respectivo énfasis en lo concerniente a la creación de una Agencia Nacional de Ciberseguridad y ciertas facultades que resultan problemáticas del mismo, así como todas las modificaciones que se le realizaron en el transcurso del debate legislativo.

Establecido los puntos posiblemente controvertidos acerca de la Agencia, un tercer capítulo busca abordar a la Comisión para el Mercado Financiero, examinando su origen, sus características y, en definitiva, la labor que ha desempeñado en torno a la ciberseguridad en los años recientes, esperando de esta forma ilustrar la duplicidad normativa entre facultades de esta y la pretendida Agencia Nacional de Ciberseguridad y la solución a la que se arribó posterior a su segundo trámite constitucional.

Un cuarto capítulo analizará el manejo que han tenido países en derecho comparado acerca de la relación que existe entre la agencia nacional y el regulador sectorial, con la finalidad de ejemplificar el dispar avance que ha tenido la materia en los Estados que han servido de inspiración, principalmente debido a la influencia que ha tenido la normativa regional de la Unión Europea (EU).

CAPÍTULO PRIMERO: EVOLUCIÓN DEL INTERNET, LA CIBERDELINCUENCIA Y LA CIBERSEGURIDAD.

1.1 EL INTERNET Y LA APARICIÓN DE LA CIBERDELINCUENCIA.

La creación de las primeras computadoras desde la década de 1930 en adelante fue un hito de relevancia mundial. Estas primitivas computadoras evolucionaron a una velocidad sorprendente en las siguientes décadas y constituirían un medio imprescindible para la posterior creación del internet en la década de 1960.

Precisamente desde el comienzo de esa década, se darían los primeros pasos para la posterior creación del internet. Dicha senda tendría su origen en la "*Defense Advanced Research Projects Agency*" (DARPA), agencia vinculada a propósitos militares e interesada en las mejoras de la comunicación, de gran relevancia en el mundo militar. En ese contexto, en 1965 se realizaría la primera conexión entre las computadoras de dos universidades norteamericanas, sin embargo, esta primitiva conexión aún no resultaba óptima para los fines propuestos[2].

Para el año 1969 la red se ampliaría, pasando de existir dos universidades interconectadas a cuatro. Además, fue en ese momento en el cual la red recibiría el nombre de "*Advanced Research Projects Agency Network*" o ARPANET, tan conocido en la cibercultura. Ahora bien, en 1972 continuaría la evolución de esta primitiva forma de internet, situación reflejada en la conformación de un entramado digital entre 50 universidades de variados estados de EE. UU. Por otro lado, no sería sino hasta un año después que comenzarían las primeras conexiones al exterior del país[3].

Durante los siguientes años continuaría el incipiente desarrollo de esta tecnología, llegando a adquirir en 1982 la denominación con la que la conocemos actualmente, esto es, Internet. Aproximadamente una década más tarde, en 1991, se produjo uno de los eventos de mayor relevancia en la materia, pues se creó la "World Wide Web" lo que supuso una interconexión a nivel global, como si efectivamente existiese una telaraña permitiendo las diversas conexiones a través del mundo. Este hito se aprecia en los números de ordenadores

[2] LÓPEZ, Manel. *Internet de las Cosas*. Rama Editorial. 2019, pp. 31. Disponible en: https://www.digitaliapublishing.com/a/110136/internet-de-las-cosas
[3] Ibid., pp. 32.

conectados, de esta forma en el periodo entre 1984 y 1989 se pasaría de 1000 conexiones a 100.000, mientras que, en el periodo posterior al mencionado hito, hubo un aumento a 1 millón de conexiones, las cuales aumentarían a 10 millones para el año 1996[4].

El crecimiento y desarrollo evidenciado se mantiene a día de hoy, abarcando una amplia gama de entornos en los que la utilización de esta tecnología es imprescindible, facilitándonos en gran medida nuestro diario vivir, ya sea a través de plataformas de comunicación, de información o incluso teniendo usos en el campo médico o espacial por nombrar algunos ejemplos. En definitiva, el Internet está presente hoy más que nunca en la mayor parte de la sociedad, moldeando nuestra forma de interactuar.

Pues bien, en el contexto de un exponencial desarrollo del Internet, no se puede evitar hablar de una situación que lo ha acompañado prácticamente desde sus inicios. Como ya se anticipó, existen ciertos individuos conocidos en la cultura popular como "*hackers*" quienes precisamente han aportado en su desarrollo identificando fallas y proponiendo soluciones. Sin embargo, un subgrupo de hackers que no cumplen esos cometidos, se han dedicado a utilizar sus conocimientos tecnológicos para obtener beneficios a partir de ataques a través del Internet. Dichos ataques, considerados delitos informáticos, pueden ser englobados dentro de la categoría de cibercrimen.

En línea con lo anterior, se ha entendido que el delito informático debe cumplir con los presupuestos de todo delito, esto es, la tipificación legal, la antijuricidad y la culpabilidad del infractor. Lo que lo diferencia es la necesidad de que se trate de un hecho cometido en contra del soporte lógico de un sistema informático o de tratamiento automatizado de información, lo cual se suele hacer a través de sistemas computacionales[5].

Por otro lado, en 2007 la Comisión Europea entendía que el cibercrimen estaba dado por actos delictivos cometidos utilizando redes de comunicaciones electrónicas y sistemas de información o en contra de tales redes y sistemas. Esta concepción llevada a la práctica implica 3 subcategorías de delitos, estos son: i) delitos tradicionales como el fraude o la falsificación; ii) publicación de contenidos ilegales como el abuso sexual infantil; y iii) delitos exclusivos de las redes electrónicas. Las características comunes entre ellos son la escala

[4] Ibid., pp. 33.
[5] VALDEZ, Aldo. *El Cibercrimen*. 2009, pp. 1. Disponible en: https://www.researchgate.net/publication/338493033_El_Cibercrimen

a la que pueden efectuarse, generalmente masiva, y la distancia entre el delito propiamente tal y sus consecuencias[6].

Sin perjuicio de las concepciones mencionadas en torno al tema, es necesario recordar que los orígenes de los delitos informáticos están ligados a la creación del internet y a la evolución de las Tecnologías de la Información y las Comunicaciones (TICs). De esta forma, uno de los primeros delitos de relevancia de esta clase fue el cometido por John Draper en EE. UU., un "*phreaker"*, denominación que proviene del neologismo entre las palabras "*freak*", "*hack*" y "*free*", categoría de *hackers* especializadas en delitos a través de líneas telefónicas[7].

En 1971, Draper descubrió una forma de realizar llamadas internacionales gratuitas utilizando una determinada frecuencia de sonido, 2600 Hz, luego de utilizar un silbato que venía en una caja de cereales, pues dicha frecuencia permitía al usuario acceder a la línea telefónica de la compañía AT&T como si fuese un operador de la misma. Más tarde desarrollaría una máquina denominada "*blue box*" que realizaba la misma función que el silbato. Por estos hechos, fue arrestado en 1972 por el cargo de fraude telefónico[8].

Pues bien, la incipiente evolución del internet y las tecnologías relacionadas supuso más y nuevas formas de cometer delitos, sobre todo teniendo en cuenta hitos posteriores como la creación del correo electrónico y los navegadores web. En el caso del correo electrónico, uno de los delitos cibernéticos más populares es el "phishing", que se produce cuando el atacante envía un correo electrónico al usuario aparentando ser de una fuente confiable, y en este incluye un enlace o archivo adjunto que induce al usuario a instalar un programa malicioso que le permitirá recolectar información confidencial de la víctima[9].

Como ya se anticipó, lo que distingue a este tipo de delitos es el hecho de que la comisión del mismo puede verificarse en un lugar completamente diferente a aquel en que se

---

[6] COMISIÓN DE LAS COMUNIDADES EUROPEAS (CCE). *Hacia una política general de lucha contra la ciberdelincuencia*. 22 de mayo de 2007, pp. 2. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0267

[7] LEMOS, André. *CIBER-REBELDES*. 2023, pp. 1. Disponible en: https://www.researchgate.net/publication/265577731_CIBER-REBELDES

[8] BEDERMAN, Uriel. *La historia de John Draper, el primer "hacker malo" que engañó a los poderosos con un silbato de juguete*. TN. [En línea], 03 de septiembre 2022. Disponible en: https://bit.ly/46DX7uL

[9] KAUR, Shubhdeep y RANDHAWA, Sukhchandan. *Dark Web: A Web of Crimes*. Wireless Personal Communications 112, 2131–2158. 2020, pp. 17. Disponible en: https://doi.org/10.1007/s11277-020-07143-2

encuentra el atacante, concretamente se producen en lo que se ha denominado "ciberespacio". Estamos hablando de un lugar abstracto, compuesto de elementos físicos, lógicos y sociales en el cual las personas se relacionan, que sigue creciendo a un ritmo acelerado a la par con la evolución tecnológica y que precisamente uno de los problemas que trae aparejado es una ausencia de fronteras físicas, lo que implica una limitación de espacio y, por otro lado, una limitación temporal, en relación con los hechos delictivos que allí se cometen[10].

En años más recientes, se estimaba que más de un tercio de la población mundial tenía acceso a internet, mientras que se esperaba que para 2020 el número de dispositivos interconectados superase la cantidad de personas en una proporción de 6 a 1[11]. Justamente en un contexto como el reseñado que denota la magnitud de la evolución que ha tenido el internet y junto a ello el cibercrimen es que se hizo necesaria una cooperación entre los diversos países alrededor del mundo con la finalidad de aminorar las consecuencias negativas que suponen este tipo de ilícitos.

Esta cooperación tiene su principal manifestación en la creación de normativa que permitiese la defensa en contra de los delitos cibernéticos, estamos hablando de una normativa integral que lamentablemente a día de hoy no ha logrado consolidarse o ha tardado en hacerlo en todas las regiones de nuestro planeta, sin embargo, ha habido importantes avances dirigidos a esa meta[12]. Uno de esos avances es el que nuestro país está teniendo actualmente al discutirse el proyecto que analizamos en este documento.

1.2 LA CIBERSEGURIDAD.

Ya advertimos que para lograr una defensa efectiva contra el cibercrimen es necesario contar con una normativa y marcos regulatorios tendientes a dicha protección, lo cual supone generar una efectiva y mejor seguridad en las redes y en los aparatos tecnológicos que utilizamos para conectarnos a dichas redes. Pues bien, la intención de contar con seguridad en ese ámbito se ha conocido como ciberseguridad, y en los inicios del Internet

[10] TEJERINA, Ofelia. Aspectos jurídicos de la ciberseguridad. Rama Editorial. 2020, pp. 47. Disponible en: https://www.digitaliapublishing.com/a/110180/aspectos-juridicos-de-la-ciberseguridad
[11] UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Estudio exhaustivo sobre el delito cibernético*. 2013, pp. 15. Disponible en: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf
[12] Ibid., pp. 17.

no se tuvo en mucha consideración o dicho de otra forma no fue uno de los principales objetivos que la primitiva forma de internet deseaba conseguir[13].

Así como el Internet, el cibercrimen y el ciberespacio han evolucionado de manera exponencial durante las últimas décadas, la misma trayectoria ha seguido la ciberseguridad. Sobre lo que no cabe duda es que se erige como el mecanismo de control del riesgo en el ciberespacio, por otro lado, entrando en más detalles, podríamos comprenderla como un conjunto de técnicas, procedimientos y protocolos que buscan lograr esa finalidad de mantener a raya el cibercrimen[14].

En ese contexto, una de las manifestaciones más relevantes en torno a la ciberseguridad en una perspectiva internacional ha sido la convención sobre cibercrimen del Consejo de Europa (CE), más conocida como el Convenio de Budapest, que además resulta ser el primer tratado internacional en la materia[15]. Se trata de un convenio que tiene sus orígenes años antes con un estudio realizado por Organización para la Cooperación y Desarrollo Económico (OCDE) relacionado con la posibilidad de armonizar las legislaciones nacionales sobre cibercrimen[16].

En el contexto de la búsqueda de una armonización, el convenio equipara al cibercrimen con la delincuencia, y ante ello los Estados parte deben contar con estrategias para enfrentar esta situación a través del sistema de justicia criminal[17]. Para llevar a cabo dicha labor, nos entrega un catálogo de situaciones que los países deben criminalizar a través de su normativa interna[18].

Por otro lado, también en el ámbito internacional, la asamblea general de la Organización de Naciones Unidas (ONU) dictó hace más de dos décadas las Resoluciones de la 55/63 (2000) y 56/121(2001), ambas tendientes a la lucha contra la utilización de la tecnología de la información con fines delictivos. Posterior a ello sobrevinieron otras dos resoluciones relacionadas con la temática, la resolución 57/239 (2002) que promueve la creación de una

---

[13] TEJERINA, Ofelia, 2020. op. Cit., pp. 91.
[14] GAYOSO, Víctor, HERNÁNDEZ, Luis y ARROYO, David. *Ciberseguridad*. CSIC, 2020. pp. 12. Disponible en: https://www.digitaliapublishing.com/a/80863/ciberseguridad
[15] CONSEJO DE EUROPA. *Convenio N.º 185 sobre la ciberdelincuencia*. 23 de noviembre de 2001. Disponible en: https://rm.coe.int/16802fa41c
[16] BRENNER, Susan. *La Convención sobre Cibercrimen del Consejo de Europa*. Revista Chilena de Derecho y Tecnología. 1 (1): pp. 221-238. 2012, pp. 226. Disponible en: https://doi.org/10.5354/0719-2584.2012.24030
[17] Ibid.
[18] Ibid., pp. 227.

cultura global de ciberseguridad y la resolución 58/199 (2004) que continuó con la promoción de la creación de una cultura mundial de seguridad cibernética y añadió además la protección de las infraestructuras de información esenciales.

Sin perjuicio de la relevancia de los documentos mencionados, la realidad es que ante el advenimiento de los delitos cibernéticos ya en la década de los ochenta había países que habían comenzado a penar este tipo de ilícitos con leyes específicas al efecto, mientras que ya en los noventa tanto en Norteamérica como en Europa se adoptaron leyes que penalizaban un conjunto de actividades que podemos incluir dentro del término cibercrimen, como por ejemplo el acceso no autorizado a sistemas informáticos[19]. En el caso de Estados Unidos, esta normativa sería la "Computer Fraud and Abuse Act" la cual denotaba el interés de la protección de los ordenadores, especialmente aquellos en los que existiese un interés federal, como es el caso de los que pertenecían a bancos.

Volviendo al contexto internacional donde ya aludimos a lo proporcionado por el CE y la ONU, es inevitable hablar de otras regulaciones provenientes de la Unión Europea (UE). En un comienzo, en el año 2000, sus intenciones se manifestaron a través de la comunicación conjunta del Consejo y de la Comisión Europea, destinada a crear una sociedad de la información más segura, mejorar la seguridad de las infraestructuras de información y la lucha contra la delincuencia informática, pues entendían que las nuevas tecnologías de la información y la comunicación estaban teniendo impacto revolucionario tanto en la economía como la sociedad de los Estados parte, y, sin embargo, no se trataba de infraestructuras invulnerables ante las conductas criminales[20].

Posterior a ello, en 2002, la Comisión propondría una decisión marco a través del Consejo relativa a los ataques de los que son objeto los sistemas de información. Nuevamente, se evidenció una preocupación por el importante papel que poseen las redes de comunicación electrónica y los sistemas de información para la comunidad europea, lo cual, por supuesto, implica ventajas, pero a la vez significa riesgos. Ante ello, la decisión trata ciertos tipos de

[19] Ibid., pp. 223.
[20] UNION EUROPEA. *COM 2000/890 final. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. 2001, pp. 2. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

ataques que pueden sufrir los sistemas de información, además otros factores relacionados[21].

Con el pasar de los años se publicarían diversos documentos por parte de la UE dedicados a la temática, lo que denota el compromiso que han tenido en promover la ciberseguridad y el desarrollo de normativa o recomendaciones atingentes a la materia, toda vez que afectan a una multitud de países, y que, en el caso del Convenio de Budapest, no resulta privativa de aquellos estados pertenecientes a la Comunidad Europea, sino que ha llegado a ser ratificado por más de 60 países alrededor del mundo.

1.3 EVOLUCIÓN HISTÓRICA DE LA CIBERSEGURIDAD EN CHILE. CONTEXTO LEGAL ACTUAL.

En Chile la llegada del Internet y de las nuevas tecnologías ligadas a su desarrollo, al igual que muchos otros países subdesarrollados, se produjo algunos años después que en aquellos países de regiones desarrolladas como Norteamérica y Europa.

Debido a esa razón es que uno de los primeros y más relevantes antecedentes de nuestro acercamiento a la materia se dio a través de las TIC en 1985, pues en dicho año se produjo el envío del primer correo electrónico entre la Universidad de Chile y la Universidad de Santiago producto de un proyecto nacional al efecto[22]. Sin embargo, la llegada del Internet como tal llegaría recién en 1992 cuando se produjo la primera conexión vía banda ancha entre Chile y EE. UU., con la particularidad de que, a diferencia de otros países en que la política era “un país, una conexión”, en nuestro país se permitieron 2 enlaces, uno para la Universidad de Chile y otro para la Universidad Católica, debido a las disputas existentes entre estas dos universidades[23].

Sin perjuicio de este hito, y dentro del ámbito del cibercrimen y por lo mismo en relación con la ciberseguridad, en julio de 1991 ya había entrado en discusión el proyecto de ley que precisamente buscaba regular los crímenes cibernéticos[24], proyecto que decantaría en 1993 en la Ley 19.223 que tipifica figuras penales relativas a la informática. La moción del

[21] UNION EUROPEA. *COM 2002/173 final. Propuesta de Decisión-marco del Consejo relativa a los ataques de los que son objeto los sistemas de información*. 2002, pp. 2. Disponible en: https://www.europarl.europa.eu/meetdocs/committees/libe/20020522/173000es.pdf
[22] CSIRT. *Día Mundial de Internet: Hitos de la llegada de internet a Chile*. [En línea] 17 de mayo de 2022, Disponible en: https://bit.ly/3M738rM
[23] Ibid.
[24] CHILE. Proyecto de ley sobre Delito Informático. Boletín 412-07. 16 de julio de 1991. Disponible en: https://bit.ly/4abNqpM

diputado Viera-Gallo, quien lo llevó a discusión, se fundaba en las mismas ideas que ya hemos observado en el ámbito internacional, es decir, se asumió el creciente desarrollo de las tecnologías de la información y los grandes beneficios que esta representa, pero a la vez se entendió que dicho desarrollo ha evidenciado lo vulnerable que puede quedar la sociedad con su uso[25].

Ahora bien, la ley aprobada y promulgada solo constó de 4 artículos que establecían una tipificación amplia de las conductas, sin entregar definiciones que pudieran ser pertinentes al efecto y penas que van desde el presidio menor en su grado mínimo a presidio menor en su grado máximo[26]. Sin perjuicio de ello, Chile tendría la primera y única ley encargada de regular lo concerniente al ciberdelito. Sin embargo, esta falta de detalles implicó que ni siquiera existiese una definición de lo que consistía el delito informático, no obstante, se entendió que la concepción que primó fue aquella según la cual se busca proteger los datos y sistemas informáticos a través del sistema penal, lo que significaba seguir un concepto restringido como el sostenido por la Organización de Naciones Unidas (ONU)[27].

Por otro lado, la doctrina se cuestionó acerca de cuál era el bien jurídico que se deseaba proteger mediante esta legislación. En ese sentido, la moción parlamentaria que originó el proyecto se refirió a la protección de la calidad, pureza e idoneidad de la información[28], sin embargo, esto hace que el bien jurídico que se busca proteger se torne genérico, distanciándose de los elementos materiales que son el objeto de ataque y a la vez de la especialidad que supone el cibercrimen[29]. En ese orden de ideas, y a pesar de las múltiples críticas que puede hacerse en contra de dicha legislación, esta mantuvo su vigencia por bastantes años, incluso teniendo en consideración la exponencial evolución de la materia, que ya se ha puesto de manifiesto con anterioridad en este documento.

Con todo, esta no ha sido la única expresión sobre el tema en nuestro país. De esta forma, resulta interesante mencionar ciertos decretos tales como el decreto supremo N.º 5996 de

---

[25] Ibid.
[26] CHILE. Ley 19.223, *Tipifica Figuras Penales Relativas a la Informática*. Diario Oficial de la República de Chile, Santiago, Chile, 17 de junio de 1993. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=30590
[27] LARA, Juan, MARTÍNEZ, Manuel y VIOLLIER, Pablo. *Hacia una regulación de los delitos informáticos basada en la evidencia*. Revista Chilena De Derecho Y Tecnología, 3(1). 2014, pp. 109. Disponible en: https://doi.org/10.5354/0719-2584.2014.32222
[28] CHILE, 1991, op. cit.
[29] MOSCOSO, Romina. *La Ley 19.223 en general y el delito de hacking en particular*. Revista Chilena de Derecho y Tecnología, 3(1). 2014, pp. 15. Disponible en: https://doi.org/10.5354/0719-2584.2014.32220

1999 que creó y puso en marcha la red interna del Estado, la cual sería luego actualizada en 2005 mediante el decreto supremo N.º 1299. También en 2005 se promulgó el decreto supremo N.º 83 que aprobó la norma técnica para los órganos de la administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos. Decretos como estos dan cuenta de la relevancia que cobraron las redes para la administración del Estado, así como también la seguridad de los documentos electrónicos que esta emitía.

Ya en el año 2015, fue promulgado el decreto N.º 533 que creó el Comité Interministerial sobre Ciberseguridad. A dicho ente se le encargó la misión de proponer una política nacional de ciberseguridad, sugerir alternativas de seguimiento a su avance e implementación, y asesorar en la coordinación de acciones, planes y programas en materia de ciberseguridad de los distintos actores públicos y privados en la materia[30]. Para el cumplimiento de tales tareas se le otorgó diversas funciones, entre las que destaca el asesoramiento al Presidente de la República, precisamente enfocado en el análisis y definición de la política nacional de ciberseguridad[31].

Justamente gracias al cumplimiento de dicha función por parte de este comité es que, en 2017, y durante el segundo mandato de la expresidenta Michelle Bachelet, el Ministerio del Interior y Seguridad Pública despachó la primera política nacional de ciberseguridad (PNCS), la que incluyó las principales preocupaciones y objetivos en torno a la ciberseguridad a tenerse en cuenta durante un periodo de 5 años, es decir, desde 2018 a 2022. En ese contexto, uno de los fines a los que aspiraba dicha política, y una meta esperable para 2022, era contar con una infraestructura de la información robusta y resiliente[32], para ello, uno de los objetivos a corto plazo fue contar con equipos de respuesta ante los incidentes de ciberseguridad, esto se lograría con la implementación de Equipos de Respuesta a Incidentes de Seguridad Informática o CSIRT (*Computer Security Incident Response Team*) al igual que lo han hecho otros países en el plano internacional.

Dentro de ese objetivo se planteó otro dedicado al reforzamiento del CSIRT de gobierno que ya existía para ese momento. Dicho reforzamiento se conseguiría en 2019 mediante la

[30] CHILE. Decreto N.º 533, *Crea Comité Interministerial sobre Ciberseguridad*. Diario Oficial de la República de Chile, Santiago, Chile, 17 de Julio de 2015. Artículo 1. Disponible en: https://bcn.cl/3gbju
[31] Ibid., Artículo 2.
[32] COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD (CIC). *Política Nacional de Ciberseguridad* (PNCS). 27 de abril de 2017, pp. 16. Disponible en: https://biblioteca.digital.gob.cl/handle/123456789/738

Resolución Exenta 5.006, que formalizaría al CSIRT de Gobierno como un Departamento dentro de su estructura, específicamente como parte integrante de la Subsecretaría del Interior y Seguridad Pública[33]. Por otro lado, aunque fue mencionado en las estrategias públicas que abordaban el tema, durante el año 2018 se crearía un cargo dentro del Gobierno denominado "Coordinador Nacional de Ciberseguridad", cuyo objetivo es liderar las discusiones e iniciativas legislativas en materia de ciberseguridad y que por tal razón jugaría un importante rol como representante del Ejecutivo en la discusión del proyecto de ley que se analizará en el próximo capítulo de este documento.

De cualquier forma, la política nacional descrita se considera el primer instrumento del Estado que tiene por objeto resguardar la seguridad de las personas y de sus derechos en el ciberespacio y su publicación supuso tres años previos de trabajo para sus creadores, quienes se vieron en complicaciones debido a falta de estudios e información sobre el estado de la seguridad digital, tanto en el sector público como privado. Es por ello que resulta de gran relevancia realizar estudios que permitan ir dilucidando los efectos que los diversos aspectos de la ciberseguridad pueden ir provocando, sobre todo teniendo en consideración que el incremento en el uso del internet y las tecnologías de la información y comunicación aumentan la vulnerabilidad de los usuarios frente a las redes[34].

Ahora bien, si queremos seguir explorando la evolución histórica de nuestro país en torno a la ciberseguridad, pero en el ámbito específico del cibercrimen, no podemos sino mencionar otro evento de relevancia acaecido también en 2017. Después de todo, fue ese mismo año en que Chile promulgó el convenio sobre la ciberdelincuencia[35], más conocido como el Convenio de Budapest. Se trata de un convenio que entró en discusión parlamentaria a través de un mensaje de la expresidenta Michelle Bachelet en 2016. Dicho instrumento comenzó a regir desde 2004 en los Estados miembros del Consejo de Europa, pero no fue sino hasta el año 2017 que Chile se hizo parte, buscando así reafirmar su posición frente al cibercrimen mediante la colaboración con el resto de países que lo han suscrito, lo cual en cierta forma se condice principalmente con uno de los objetivos

[33] CSIRT. *Chile formaliza creación del CSIRT de Gobierno*. [En línea], 1 de septiembre de 2019. Disponible en: https://www.csirt.gob.cl/noticias/chile-formaliza-creacion-del-csirt-de-gobierno/
[34] ÁLVAREZ, Daniel. *Los desafíos de la ciberseguridad en Chile*. Revista Chilena De Derecho Y Tecnología, 6(2), 1–2. 2017. Disponible en: https://doi.org/10.5354/0719-2584.2017.48027
[35] CHILE. Decreto N.º 83, *Promulga el Convenio sobre la Ciberdelincuencia*. Diario Oficial de la República de Chile, Santiago de Chile, 28 de agosto de 2017. Disponible en: https://bcn.cl/2ij3n

establecidos en la PNCS, esto es, el establecimiento de relaciones de cooperación en ciberseguridad con otros actores[36].

Pues bien, a partir del preámbulo del convenio[37] se establece que este es "necesario para prevenir los actos que pongan en peligro la 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".

A pesar de la promulgación mencionada, esto no produjo cambios inmediatos en nuestra normativa. Es más, a la fecha la promulgación nacional del Convenio, nuestra normativa interna en relación con delitos informáticos (Ley N.º 19233) era bastante escueta y sin mucho detalle, de tal forma que este instrumento vino de alguna forma a enriquecer nuestros conocimientos en la materia, razón por la cual en 2018 mediante mensaje del expresidente Sebastián Piñera se ingresó un proyecto que tenía por finalidad establecer normas sobre delitos informáticos, así como derogar la ley N.º 19.223 y modificar otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest[38].

Algunas de las razones esgrimidas en el mensaje dicen relación con el impacto del internet en la población chilena, además del compromiso adquirido por el gobierno de turno a través del programa "Construyamos tiempos mejores para Chile" en torno a actualizar la ley de delitos informáticos. Se dejó constancia de que la Ley 19.233 no había sufrido modificaciones desde su dictación en 1993, época en la que el internet era un fenómeno incipiente y de escaso acceso, y en ese mismo contexto, las herramientas de persecución penal que datan desde la dictación del Código Procesal Penal en el 2000 se han vuelto ineficaces frente a las nuevas formas de delitos[39]. Aunado a ello, la actualización de la

[36] CISC, 2017, op. cit., pp. 22.
[37] CE, 2001, op. cit., pp. 2.
[38] CHILE. Proyecto de ley que establece normas sobre Delitos Informáticos, deroga la Ley N.º 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Boletín N.º 12.192-25, 25 de octubre de 2018. Disponible en: https://bit.ly/48awTR1
[39] Ibid., pp. 3.

normativa sobre delitos informáticos también es uno de los objetivos dispuesto por la PNCS[40].

Como resultado de la deliberación parlamentaria, en 2022, se publicaría la Ley N.º 21.459 con las finalidades ya mencionadas, la cual representa un gran salto en comparación a la regulación existente a la fecha. De esta forma, a diferencia de la antigua ley, se comienza entregando algunas definiciones claves en torno a la ciberdelincuencia, las que fueron inspiradas por el Convenio, tales como: acceso ilícito, falsificación informática, fraude informático, entre otros. Por otro lado, supone un avance al contener normas relativas al procedimiento aplicable en el caso de incumplimiento de las disposiciones que establece, lo que denota la especialidad en ciertos aspectos que tiene esta materia en relación con las normas procesales generales[41].

Con esto establecido, hemos hecho un breve repaso por algunas de las principales normas vigentes tanto respecto del cibercrimen como de la ciberseguridad nacional, sin embargo, aunque ha habido avances significativos, aún hace falta cumplir algunos de los desafíos que supuso la PNCS en 2017 o al menos lograr un mayor nivel de cumplimiento de los mismos. Entre ellos resulta imperativo el referido a contar con una infraestructura de la información robusta y resiliente, lo cual en parte se traduce en contar con una institucionalidad y modelo de gobernanza de la ciberseguridad tendiente a un desempeño coordinado de funciones[42]. Esta idea de contar con una gobernanza y una institucionalidad tuvo un desarrollo relevante en 2022, puesto que, antes de acabar el segundo mandato del expresidente Sebastián Piñera, se despachó un proyecto de ley al senado al efecto. Este proyecto se denominaría “Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información”, proyecto de relevancia para el estado actual y futuro de la ciberseguridad en Chile y que será objeto de análisis en el siguiente capítulo de este documento.

[40] CISC, 2017, op. cit., pp. 27.
[41] CHILE. Ley 21.459, *que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest*. Diario Oficial de la República de Chile, Santiago de Chile, 20 de junio de 2022. Disponible en: https://bcn.cl/32uaf
[42] CIC, 2017. op. cit., pp. 25.

CAPÍTULO SEGUNDO: PROYECTO DE LEY MARCO SOBRE CIBERSEGURIDAD E INFRAESTRUCTURA CRÍTICA DE LA INFORMACIÓN.

2.1 ORIGEN DEL PROYECTO.

En marzo de 2022, mediante mensaje[43] del en ese entonces presidente de la República, Sebastián Piñera, se presentó al Senado el Proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información, Boletín N° 14.847-06. La intención detrás de la presentación de este proyecto era "establecer la institucionalidad necesaria para robustecer la ciberseguridad, ampliar y fortalecer el trabajo preventivo, la formación de una cultura pública en materia de seguridad digital, enfrentar las contingencias en el sector público y privado, y resguardar la seguridad de las personas en el ciberespacio"[44], objetivos que de alguna forma se habían anticipado ya en la PNCS de 2017. Actualmente, el proyecto ya pasó por su primer trámite constitucional en el Senado y se encuentra en su segundo tras ser objeto de deliberación por diversas comisiones técnicas.

El artículo 1 del proyecto despachado por el Senado dispone que:

"La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones privadas, y los mecanismos de control, supervisión y de responsabilidad ante infracciones…"[45]

En ese sentido, el primer artículo nos da a entender que el objetivo del proyecto es materializar los avances que durante los años anteriores y mientras seguía vigente la PNCS no se habían logrado concretar, más específicamente en lo relativo a la gobernanza pública en materia de ciberseguridad[46].

---

[43] CHILE, 2022, op. cit.
[44] Ibid., pp. 6.
[45] COMISIÓN DE SEGURIDAD CIUDADANA (CSC). *Comparado Segundo Trámite Constitucional, sobre el Proyecto de Ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información* (Boletín N.º 14.847-06). 10 de mayo de 2023a, pp. 1. Artículo 1.
[46] ÁLVAREZ, Daniel. *Agenda legislativa sobre ciberseguridad en Chile*. Revista Chilena De Derecho Y Tecnología, 7(2), 1–3. 2018, pp. 3. Disponible en: https://doi.org/10.5354/0719-2584.2018.51992

Al respecto podríamos mencionar ciertos hechos que lograron de alguna manera cimentar el camino para llegar a discutirse el proyecto objeto de este trabajo. Claramente, uno de ellos es la PNCS a la cual ya nos hemos referido, sin embargo, si tuviésemos que hablar de cambios materiales en virtud del cumplimiento de los objetivos de dicha política podríamos señalar la Ley N.º 21.113 de 2018 que declara el mes de octubre como el mes nacional de la ciberseguridad, la cual no solo constituye una representación simbólica significativa, sino que también promueve la coordinación en el desarrollo de actividades de concienciación sobre seguridad digital, tanto en el sector público como en el privado, contribuyendo de esta manera al fortalecimiento de los niveles de madurez organizacional en Chile[47].

En segundo lugar, desde 2017 se ha discutido en el Congreso el proyecto de ley sobre datos personales que necesariamente se espera forme parte de los pilares del marco jurídico de la ciberseguridad en nuestro país[48]. Se trata de un proyecto que incorpora la seguridad en el tratamiento de datos personales como un principio rector y como un deber de información y transparencia respecto a las políticas y medidas adoptadas por la organización, además de añadir otros objetivos al respecto.

Por otro lado, también puede resultar relevante mencionar el proyecto de ley de 2018 que modificó la ley de bases de los Procedimientos Administrativos en materia de documentos electrónicos[49], la cual decantó en 2019 en la publicación de la Ley 21.180, denominada “Ley de transformación digital del Estado”, puesto que dicha normativa supuso ventajas para el desarrollo electrónico y digital del Estado, lo cual se apreció de forma práctica los años subsiguientes, sobre todo debido a la pandemia del COVID-19 y las medidas de confinamiento que esta produjo. Por último, y aunque ya lo hemos mencionado en el apartado anterior, la Ley 21.459, desde el punto de vista del cibercrimen o delitos informáticos, de igual modo forma parte de las modificaciones normativas que antecedieron al actual proyecto en análisis.

[47] Ibid., pp. 1.
[48] COMISIÓN DESAFÍOS DEL FUTURO, CIENCIA, TECNOLOGÍA E INNOVACIÓN (CDFCTE). *Construyendo la ciberseguridad en chile*. Ediciones Biblioteca del Congreso Nacional de Chile. 2023, pp. 17. Disponible en: https://bit.ly/46Re6t6
[49] CHILE. Proyecto de ley que modifica la Ley que establece Bases de los Procedimientos Administrativos, en materia de documentos electrónicos. Boletín N.º 11882-06. 6 de julio de 2018. Disponible en: https://bit.ly/485JoxT

2.2 ESTRUCTURA Y DISPOSICIONES GENERALES DEL PROYECTO.

El proyecto en análisis cuenta con 48 artículos, divididos en 10 títulos, así como también 8 artículos transitorios. El primer título aborda las disposiciones generales, dentro de las cuales establecen los objetivos de la ley, ya mencionados en su artículo 1, además de referirse a una cantidad de 27 definiciones de conceptos claves en torno a la ciberseguridad, de entre los cuales destacan[50]:

"*7. Ciberespacio: ambiente formado por la interconexión e interrelación compleja entre las redes y sistemas informáticos, los componentes lógicos de la información, los datos almacenados, procesados o transmitidos y las interacciones sociales que ocurren en aquel*".

"*9. Ciberseguridad: preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad*".

Se trata de definiciones relevantes, puesto que la doctrina al referirse a los mismos ha señalado la dificultad inherente de definir un concepto que está en constante cambio. Por otro lado, el proyecto resulta pionero al añadir dichas definiciones, las cuales no se encontraban en los instrumentos reseñados con anterioridad en este documento, ni siquiera en el Convenio de Budapest, que resulta tan relevante en la materia. Además de lo anterior, el título de disposiciones generales establece una serie de principios que deberán observarse en el cumplimiento de la ley.

El título segundo abarca las obligaciones en materia de ciberseguridad. De relevancia resulta el párrafo referido a los servicios esenciales y los operadores de importancia vital, pues es a ellos a los cuales en principio estaría dirigida la legislación. El artículo 4 del proyecto despachado del Senado establecía que la labor de determinación respecto de cuáles serán dichos servicios esenciales u operadores de importancia vital quedara en manos de la "Agencia", la cual "debía atender a la entidad del impacto cuya afectación o interrupción podría tener en la defensa nacional o en el mantenimiento de actividades sociales y económicas fundamentales" con el fin de realizar la mencionada determinación, incluyendo además otros criterios que el mismo proyecto establece. Aunado a lo anterior

[50] CSC, 2023a, op. cit. pp. 2-7. Artículo 2.

se establecen los deberes generales, ya sea para los organismos del estado o los servicios u operadores ya mencionados.

En el título tercero es tratada la Agencia Nacional de Ciberseguridad y los aspectos de relevancia que la rodean, como su dirección, su patrimonio, etc. El título incluye además la creación de otros dos entes, uno de ellos es el Consejo Multisectorial sobre Ciberseguridad con sus correspondientes características y el otro un CSIRT nacional que funcionará al interior de la Agencia al que se le asigna determinadas funciones.

Entre los siguientes títulos tenemos el cuarto que se refiere esencialmente a otras instituciones intervinientes (CSIRT sectoriales). El titulo quinto dedicado al CSIRT de la Defensa Nacional, el sexto en que se trata la reserva de información en el sector público en materia de ciberseguridad, el séptimo que contiene disposiciones sobre infracciones y sanciones, el octavo por su parte dispone sobre la creación de un Comité Interministerial de Ciberseguridad. Por otro lado, los títulos restantes, esto es, el noveno y décimo, tratan el cumplimiento de la normativa que se propone por parte de los organismos autónomos constitucionales, así como las modificaciones que supondría el proyecto en otros cuerpos legales, respectivamente. Finalmente se establecen una serie de disposiciones transitorias para dar cumplimiento a la ley.

2.3 LA AGENCIA NACIONAL DE CIBERSEGURIDAD Y LA EVOLUCIÓN DE SUS FACULTADES.

2.3.1 INSPIRACIÓN Y APRECIACIONES DEL ARTÍCULO QUE CREA LA AGENCIA.

Como ya se anticipó en el apartado en el que se revisó el desarrollo que ha tenido nuestro país en la materia, en Chile no contamos con un ente técnico especializado, es por ello que, siguiendo la experiencia que nos puede ofrecer el contexto internacional, así como también esperando cumplir los desafíos de nuestra propia política de ciberseguridad, el proyecto ha incluido la creación de un ente especializado, esto es, la Agencia Nacional de Ciberseguridad (ANCI).

En el contexto europeo, ya desde 2004[51], con motivo del crecimiento de las redes de comunicación y los sistemas de información, así como también el aumento de los fallos de

[51] UNIÓN EUROPEA (UE). *Reglamento (CE) N° 460/2004 del parlamento europeo y del consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Informació*n. Diario Oficial de la Unión Europea, 13 de Marzo de 2004. Disponible en: http://data.europa.eu/eli/reg/2004/460/oj

seguridad que provocaban gran desconfianza de los usuarios y el propio desarrollo del comercio electrónico, es que la Unión Europea (UE) decide tomar cartas en el asunto y dictar un reglamento al respecto[52].

Dicho reglamento dio origen a la "Agencia Europea de Seguridad de las Redes y de la Información (conocida como ENISA por sus siglas en inglés), cuya finalidad general se abocaba a garantizar, tanto para los ciudadanos, consumidores, empresas e instituciones públicas un nivel efectivo y elevado de seguridad de las redes y de la información en la comunidad. Aunado a ello, está la idea de fomentar una cultura de la seguridad de las redes y de la información en la Unión Europea[53].

Posteriormente en el año 2013[54], el reglamento mencionado fue derogado, ello en virtud de su obsolescencia, a la luz de los nuevos retos que supuso la protección de las redes y la información, así como también de la evolución de tecnología en el ámbito socioeconómico. Estos nuevos retos implicaron que el establecimiento del nuevo reglamento tuviera como objetivo principal robustecer a la Agencia, de forma que esta fuera capaz de alcanzar los objetivos propuestos y afrontar además los nuevos desafíos que conlleva la variable materia de la seguridad en las redes y la información[55].

No se necesitaría el paso de muchos años para que en 2019[56] nuevamente hubiese una modificación en torno al tema, ¿las razones?, similares a las ya comentadas, las TICs se convirtieron en el pilar de complejos sistemas que guían el comportamiento diario de las personas y la sociedad en la que se desenvuelven, de esta forma, la digitalización y la conectividad se transformó en un componente inherente a gran parte de los productos y servicios, implicando un aumento exponencial de dispositivos conectados así como un aumento en la exposición de los usuarios al riesgo de ser víctima de un delito informático[57].

---

[52] Ibid., pp. 1.
[53] Ibid., pp. 4. Artículo 1.
[54] UNIÓN EUROPEA (UE). *Reglamento (UE) N° 526/2013 del parlamento europeo y del consejo, de 21 de mayo de 2013, relativo a la agencia de seguridad de las redes de la información de la unión europea (ENISA) y por el que se deroga el reglamento (CE) N° 460/2004*. Diario Oficial de la Unión Europea, 18 de Junio de 2013. Disponible en: http://data.europa.eu/eli/reg/2013/526
[55] Ibid., pp. 2.
[56] UNIÓN EUROPEA (UE). *Reglamento (UE) 2019/881 del parlamento europeo y del consejo, de 17 de abril de 2019, Relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la Ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) N° 526/2013* («Reglamento sobre la Ciberseguridad»). Disponible en: http://data.europa.eu/eli/reg/2019/881/oj
[57] Ibid., pp. 1.

Pues bien, el proyecto en análisis supuso el estudio de 14 países que han logrado avances en la materia, dos de los cuales serán tratados en un apartado posterior de este documento. Lo que sí es posible adelantar es que existe una importante influencia de la experiencia europea, incluso en lo concerniente a la creación de la Agencia como la que pretenden nuestros legisladores[58].

Dicho lo anterior, en el mensaje emitido por el expresidente Sebastián Piñera, es el título III del proyecto, concretamente el artículo 8° el que crea esta institución, caracterizándola de la siguiente forma:

"…un servicio público funcionalmente descentralizado, dotado de personalidad jurídica y patrimonio propios, de carácter técnico y especializado, cuyo objeto será asesorar al Presidente de la República en materias propias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones con competencia en materia de ciberseguridad y regular y fiscalizar las acciones de los órganos de la Administración del Estado y privados que no se encuentren sometidos a la competencia de un regulador o fiscalizador sectorial, y que posea infraestructura de la información calificada como crítica, según los preceptos de esta ley…"[59]

En el proceso de discusión en el Senado[60], este artículo fue objeto de modificaciones por parte del asesor del Poder Ejecutivo relacionadas con la ampliación de los objetivos de la Agencia, incluyendo el velar por la protección, promoción y respeto del derecho a la seguridad informática, añadiendo además a la labor de coordinar la labor de supervisar, la cual no se verificaría sobre "instituciones con competencia en materia de ciberseguridad" sino que sobre "organismos de la Administración del Estado en materia de ciberseguridad"[61].

Por otro lado, a diferencia de lo establecido en el mensaje, la reforma realizada por el Ejecutivo implicó la creación de un segundo inciso en el que se trata las facultades

[58] OLMOS, Renato. *Los referentes internacionales del proyecto de ley marco de ciberseguridad*. Diario Financiero. [En línea], 31 de marzo de 2023. Disponible en: https://bit.ly/3TjOIcq
[59] CHILE, 2022, op. cit. pp. 24. Artículo 8.
[60] COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS (CDNSPU). *Segundo informe de las recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información. Boletín N° 14847-06*. 20 de Abril de 2023, pp. 70. Disponible en: https://bit.ly/3Tkk02F
[61] Ibid.

regulatorias y fiscalizadoras de la agencia, incluyéndose además las sancionatorias, que el mensaje no manifestaba. Con esta nueva formulación, estas facultades se verificarían sobre los organismos de la administración del Estado e instituciones privadas en materia de ciberseguridad, se añade asimismo en este segundo inciso la facultad de la agencia de impartir instrucciones generales y particulares[62]. En esta enmienda se optó por referirse a instituciones privadas a secas, producto de que los artículos 1° y 4°, igualmente enmendados, ya aluden al deber de la agencia de determinar cuándo un privado es considerado "infraestructura crítica" o más bien, un "operador de importancia vital"[63].

Un tercer inciso propuesto por el Ejecutivo, inexistente en el mensaje, añade el deber de la agencia de velar por la coherencia normativa, con la finalidad de que sus acciones se inserten de manera armónica en el ordenamiento regulatorio y sancionatorio nacional[64].

Gran relevancia tienen las características mencionadas para el análisis posterior sobre la Comisión para el Mercado Financiero, pues vemos que se establecen una serie de facultades generales para la agencia como el asesoramiento, colaboración, coordinación, protección, promoción y respeto del derecho a la seguridad informática, supervisión, regulación, fiscalización e incluso facultad sancionatoria, facultades que bajo nuestra normativa actual no serían privativas de un organismo como el que se pretende.

Por otro lado, llama la atención los sujetos a los que la normativa se dirige, esto es, los regulados. Ya anticipábamos al revisar la estructura, que se modificó la forma en la que se hacía referencia a los privados desde el primer artículo. El texto da a entender que será aplicable a los privados cuando estos sean servicios esenciales u operadores de importancia vital, en ese sentido ya se puede prevenir que instituciones privadas tales como bancos o aseguradoras, actuales regulados por la CMF, por las labores que ejecutan podrían estar sujetos a esta normativa, cuestión que no estaría exenta de incógnitas que serán tratadas con mayor profundidad en el capítulo siguiente de este ensayo.

2.3.2 EVOLUCIÓN DE ALGUNAS DE LAS FACULTADES DE LA ANCI.

El mensaje del proyecto prosigue con el artículo 9°, el cual está dedicado a las atribuciones de las que podría, eventualmente, disponer la agencia. Se analizarán aquellas que puedan tener implicancias para los objetivos de este documento, revisando, si fuese pertinente,

[62] Ibid.
[63] Ibid., pp. 11-16 y 49-55.
[64] Ibid., pp. 70.

tanto su versión original como la posible enmienda que hayan sufrido en el contexto del primer trámite constitucional en el Senado.

Antes de aquello, conviene tener presente lo establecido en los artículos 5°, 6° y 7° del texto aprobado por el Senado y despachado ante la Honorable Cámara de Diputados, pues se trata de artículos que imponen deberes generales, específicos y, además, el deber de reportar, respectivamente. Estos deberes a los que son sometidos los regulados a los que está dirigido el proyecto podrían tener repercusiones, por ejemplo, en el caso del artículo 7 sobre el deber de reportar que fue motivo de enmienda por parte del Ejecutivo durante su discusión, dispone – en lo que se considera pertinente – lo siguiente:

"Todas las instituciones, sean públicas o privadas, e independiente de si son o no operadores de servicios esenciales, con la sola excepción de aquellos que la Agencia hubiere eximido expresamente en sus instrucciones generales o particulares, tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos, de conformidad con el artículo 23. Ello, sin perjuicio de las excepciones dispuestas en el Título V de la presente ley.

La obligación de reportar deberá cumplirse en un plazo inferior a tres horas contadas desde que se tuvo conocimiento del evento respectivo. La entidad informante podrá solicitar la prórroga de dicho plazo por una sola vez y mientras se encuentre este vigente, con la sola finalidad de recabar mayores antecedentes"[65].

Lo que resulta curioso del artículo es la extensión de su aplicación, pues, a diferencia de los deberes generales y específicos, aquí se establece un deber que no solo está dirigido a los regulados ya establecidos con anterioridad en el proyecto, sino que se trata de un deber aplicable a todas las instituciones públicas o privadas sin importar si se trata o no de un operador de importancia vital o de un servicio esencial. Por otro lado, se establece una limitación temporal para realizar el exigido reporte, aspecto que, como ya se ha mencionado, conviene tener en cuenta en apartados posteriores de este ensayo.

Respecto de las atribuciones establecidas en el proyecto, lo que resalta a primera vista es la cantidad de las mismas. En el mensaje original, nos encontrábamos con facultades aludidas en literales desde la a) hasta la p), es decir, un total de 16 atribuciones[66]. Por el

[65] CDNSPU, 2023, op. cit. pp. 68.
[66] CHILE, 2022, op. cit. pp. 24-26. Artículo 9.

contrario, el texto aprobado por el Senado posterior a su discusión concluyó conteniendo literales desde la a) hasta la y), contando así con un total de 26 atribuciones[67].

De las múltiples atribuciones establecidas, y para los objetivos del presente documento, es menester analizar algunas en particular, puesto que precisamente son aquellas las que generan inquietudes en virtud de la normativa actual en torno a ciberseguridad. En primer lugar, la letra b) del artículo 9° dispone lo siguiente:

"*b) Dictar las disposiciones para la aplicación y el cumplimiento de las leyes y reglamentos y, en general, dictar protocolos y estándares técnicos, instrucciones generales y particulares de carácter obligatorias a las instituciones públicas y privadas, con el objeto de regular los requisitos mínimos para la prevención, contención, resolución y respuesta de incidentes de ciberseguridad*"[68]

Lo relevante de este inciso gira en torno a la atribución de dictar disposiciones con la finalidad de la aplicación y el cumplimiento de leyes y reglamentos, así lo planteó el Ejecutivo en su momento, buscando dejar claramente establecida dicha posibilidad[69]. En el mensaje original, por su parte, esta disposición solo aludía a la facultad de dictar normas técnicas de carácter general y los estándares mínimos de ciberseguridad e impartir instrucciones particulares para los órganos de la Administración del Estado y para los privados, respecto de estos últimos se repetía la formulación que los incluía únicamente si se trataba de un organismo privado con infraestructura crítica y que no estuviese sometido a un regulador sectorial[70]. Dicho lo anterior, la expresión del texto aprobado por el Senado solo se refiere a instituciones públicas y privadas, sin determinar si tratándose de las privadas, estas deben ser operadores de importancia vital o no. De la falta de claridad al respecto se entiende que es aplicable de manera general.

Continuando con el análisis del artículo 9° corresponde examinar lo establecido en el literal e), que establece lo siguiente:

[67] CSC, 2023a, pp. 19-25. Artículo 9.
[68] Ibid., pp 19. Artículo 9, letra b.
[69] CDNSPU, 2023, op. cit. pp. 72.
[70] CHILE, 2022. Op. Cit. pp. 24. Artículo 9, letra b.

"*e) Establecer una coordinación con el CSIRT de la Defensa Nacional, en lo relativo a los estándares y tiempos de comunicación de incidentes de ciberseguridad o vulnerabilidades, así como respecto a las materias que serán objeto de intercambio de información*"[71].

En su versión original este literal se refería a la administración de un registro nacional de incidentes de ciberseguridad[72], sin embargo, el Ejecutivo en la discusión parlamentaria propuso el cambio del literal e) primitivo por el actual, relegando el original al literal siguiente, es decir, el literal f)[73]. Lo rescatable de esta disposición dice relación con lo que ya se anticipaba al hablar del artículo 7 y el deber de reportar que este establecía. No cabe duda de que es necesaria una coordinación entre el CSIRT de la Defensa Nacional y la Agencia, sin embargo, apreciaremos que la facultad de recibir los reportes de incidentes, no sería privativa de la Agencia, ni tampoco a los CSIRT's sectoriales que eventualmente puedan existir, de manera que quizá sean necesarios ajustes en lo que se refiere a cómo será la coordinación que se espera exista entre las entidades que la ley crea y las que existiendo antes que ellas ya se abocan a objetivos similares.

A continuación, un literal que merece cierto detenimiento es la letra g) del artículo 9no que establece lo siguiente:

"*g) Elaborar y actualizar la lista de servicios esenciales y operadores de importancia vital, en la forma prevista en el artículo 4° de la presente ley*"[74].

La razón por la cual este artículo podría generar confusión dice razón principalmente con la constante evolución que se observa en la materia, de esta forma nos podemos hacer las siguientes preguntas ¿Qué es un servicio esencial? ¿Cuándo se considera que un servicio sea dependiente de las redes y servicios informáticos? ¿Dicha dependencia debe ser total? ¿Cómo medir correctamente el impacto que tendría un incidente cuando los servicios que nos ofrece la tecnología actual son tan variados? El proyecto nos indica una definición de lo que es un servicio esencial, caracterizándolo como aquel cuya afectación o interrupción tendría un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía[75], sin embargo, con posterioridad el artículo 4 nos entrega una serie

[71] CSC, 2023a, op. cit. pp 20. Artículo 9, letra e.
[72] CHILE, 2022, op. cit. pp. 25. Artículo 9, letra e.
[73] CDNSPU, 2023, op. cit. pp. 76.
[74] CSC, 2023a, op. cit. pp 20. Artículo 9, letra g.
[75] Ibid. pp. 6. Artículo 2, numeral 25.

de criterios para la identificación de dicho servicio, ante lo cual la definición inicial se torna muy general.

Otra disposición del artículo 9° que vale la pena examinar es la establecida en el literal j, que determina lo siguiente:

"*j) Requerir a los organismos del Estado y a las instituciones privadas cualquier documento, antecedente o información que sea necesario para el cumplimiento de sus fines, incluyendo el acceso a redes y sistemas informáticos, observando de manera estricta el deber de reserva que esta ley impone, así como los consagrados por la ley N°19.628, sobre protección de la vida privada*"[76].

Lo destacable en torno a este literal dice relación con la facultad de requerir los antecedentes o información por parte de los organismos, ya sean estatales o privados, a los cuales el proyecto busca regular. Nuevamente, es preciso observar que la Agencia pretendida no sería el único ente capaz de requerir antecedentes de sus regulados, puesto que en sus facultades de fiscalización existen otras instituciones que pueden exigir estos requerimientos, como veremos más adelante. Un ejemplo de esto está dado por lo establecido a propósito del proyecto de ley que crea la "Agencia de Protección de Datos Personales", el cual establece que, en su facultad de fiscalización, dicha entidad podrá requerir documentos, libros o antecedentes que tenga el responsable del tratamiento de datos[77].

La exposición de los literales precedentes, junto con algunas observaciones de los mismos, dan cuenta de que existía una necesidad de que los parlamentarios analizaran el panorama completo y en función de ello realizaran las adecuaciones que pudieran resultar pertinentes, siempre recordando la importancia que tiene el proyecto de ley para nuestro país, y sobre todo teniendo en cuenta las múltiples áreas en las que la ciberseguridad ha cobrado especial relevancia en los últimos años.

2.3.3 MODIFICACIONES DEL SEGUNDO TRÁMITE CONSTITUCIONAL.

Como ya se indicó, el análisis efectuado a ciertas atribuciones de las que dispondría la ANCI estaba basado en las normas provenientes del texto aprobado en general por el

[76] Ibid., pp. 21. Artículo 9, letra j.
[77] CHILE. Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N°11.144-07. Marzo del 2017. Artículo 30 bis, letra c. Disponible en: https://bit.ly/3fb3knt

Senado en abril de 2023, el cual a su vez introdujo ciertas modificaciones en comparación con el mensaje presidencial que le dio origen, como ya hemos podido observar.

En su segundo trámite constitucional ante la Honorable Cámara de Diputados el proyecto fue enviado a la Comisión de Seguridad Nacional para su discusión en particular, la cual en un periodo de aproximadamente 6 meses estableció una serie de modificaciones, algunas de ellas producto de indicaciones nacidas en el seno mismo de la comisión, así como otras provenientes de indicaciones del Poder Ejecutivo, el cual ha demostrado un compromiso con el avance del proyecto, que se evidencia en la urgencia suma del mismo. La finalidad de este apartado es mostrar algunas de estas reformas, sobre todo aquellas que afectan el análisis o menciones ya efectuadas a ciertos preceptos del proyecto.

Producto del acuerdo entre los asesores parlamentarios y los representantes del Ejecutivo en las mesas técnicas al efecto, el proyecto sufrió diversas reformas que corresponde mencionar. En primer lugar, la estructura global del proyecto no presento muchos cambios, manteniéndose las denominaciones de cada título invariables a excepción del título cuarto que deja de llamarse "Otras instituciones intervinientes" para ser conocido como "Coordinación regulatoria y otras disposiciones"[78], aspecto que resultará de relevancia cuando se trate a la Comisión para el Mercado Financiero.

En cuanto al articulado propiamente tal, el artículo 1° que define el alcance que tendría la ley fue objeto de múltiples indicaciones y fuente de inquietudes entre los Diputados producto de que se trata de la norma que determina a quienes se les aplicaría la ley, y entre ellos se encontrarían las empresas privadas, instituciones respecto de las cuales se cuestionaba la aplicación tratándose de pequeñas y medianas empresas de manera que ciertos diputados exigían mayor especificación en la norma[79]. La solución se encontraría en la indicación acordada entre el Ejecutivo y los parlamentarios, indicación que evitaba hablar de empresas privadas utilizando la expresión "instituciones determinadas en el artículo 4"[80].

Por otro lado, ya aludíamos al artículo 2° dedicado a definir ciertos conceptos que tendrían utilización en la propuesta legal, precepto que luego de su paso por el Senado abarcaría un total de 27 definiciones. En su segundo trámite, esta disposición fue modificada de tal forma

[78] CSC. *Informe de la comisión de seguridad ciudadana recaído en el proyecto de ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, boletín N.º 14.847-06*. 27 de noviembre de 2023b. pp. 70. Disponible en: https://bit.ly/3TmeaxI
[79] Ibid., pp. 23.
[80] Ibid., pp. 24.

que disminuyó la cantidad de numerales a 15. Esta corrección cumple un doble propósito, el primero dice relación con la necesidad de crear una ley que sea más comprensible para el regulado, mientras que el segundo busca determinar desde un comienzo cuáles serán los conceptos realmente relevantes, toda vez que se observó durante las sesiones que no todos los que provenían del texto del Senado volvían a mencionarse a lo largo del proyecto. En otro orden de ideas, existía cierta preocupación por aquellas definiciones que pudiesen estar ligadas a ciertas tecnologías afectas a mutar con el paso del tiempo, lo cual podría devenir en una obsolescencia de las mismas[81]. Precisamente una de las definiciones que resultaron suprimidas fue la de "ciberespacio" ya mencionada con anterioridad.

Posteriormente, el artículo 4° referido a la determinación de los servicios esenciales y operadores de importancia vital, y caracterizado por su extensión, también fue objeto de modificaciones, esta vez producto de indicaciones provenientes del Ejecutivo[82]. En apartados anteriores de este documento se aludió al mismo, criticando la generalidad con la que esperaba definir cuáles son los servicios esenciales, lo cual estaría dado por diversos criterios que allí se mencionaban y que tendrían que ser analizados por la Agencia como parte de sus atribuciones. La indicación del Ejecutivo al respecto transformó aquello y el nuevo artículo 4° se refiere al ámbito de aplicación de la ley, dedicando los incisos segundo y tercero del mismo a determinar cuáles serán las instituciones que presten servicios calificados de esenciales, entre ellos se consideran de forma expresa la infraestructura de la banca, servicios financieros y medios de pago, que resultan relevantes respecto del análisis que se efectuará sobre la Comisión para el Mercado Financiero que actúa como regulador sectorial respecto de dichos servicios.

Sin perjuicio de este cambio, los expertos mantenían inquietudes relacionadas, al igual que se apreciaba en la formulación anterior, con la generalidad del nuevo artículo, toda vez que en el segundo inciso del mismo se mencionan sectores de regulación tales como "servicios de tecnología de la información" que necesariamente abarcarían una gran cantidad de sujetos regulados, es decir, se trata de menciones muy amplias que podrían eventualmente afectar la certeza jurídica[83]. Con las recomendaciones de los expertos, además de la

[81] CSC. Explicaciones de Michelle Bordachar, asesora jurídica y legislativa del coordinador nacional de ciberseguridad. Sesión de la comisión del 27 de septiembre de 2023. [En línea], Disponible en: https://www.camara.cl/prensa/television.aspx
[82] SECRETARIA GENERAL DE LA PRESIDENCIA (SGP). *Oficio N° 170-371*. 26 de septiembre de 2023a. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32413&prmTIPO=OFICIOPLEY
[83] CSC. Opinión de Claudio Magliona, abogado experto en ciberseguridad. Sesión de la comisión del 27 de septiembre de 2023.

discusión y su posterior acuerdo en la propia comisión se determinó que para subsanar esta problemática se añadiese un inciso final al artículo 4° propuesto, dicha indicación provenía de una orientación previa realizada por el Ejecutivo según la cual la Agencia identificaría mediante una resolución exenta aquellas infraestructuras que serán calificados de esenciales y que quedaran sujetas a las obligaciones que la ley establece.

Producto de la extensión del artículo 4° propuesto por el Senado, el Ejecutivo propondría dos nuevos artículos, incluyendo en ellos parte del contenido que establecía el mismo previo a la reforma aludida, y que reemplazarían a los que constituían el 5° y 6°. De esta forma, y a grandes rasgos, el nuevo artículo 5° abarcaría los criterios y forma de establecer o determinar cuáles serán los operadores de importancia vital, mientras que el nuevo artículo 6° trataría el procedimiento de calificación de los operadores de importancia vital y la procedencia de recurso en contra de dicha calificación por parte de los regulados. Esta última situación fue objeto de inquietud por parte de los parlamentarios en sesiones previas, lo que devino en alteraciones de su contenido, pasando de la sola procedencia del recurso de reposición a admitir todos los recursos a los que faculta la Ley N.º 19.880[84], sin perjuicio del recurso de reclamación judicial que el propio proyecto establece.

Esta inclusión de dos artículos nuevos modificó la numeración de los siguientes en la forma que fueron despachados desde el Senado, de manera que el artículo 8° en que se daba a conocer a la Agencia se trasladó al artículo 10°, mientras que el artículo 9° relativo a las atribuciones de la misma se trasladó al artículo 11°. Precisamente el nuevo artículo 9° sería discutido en la comisión a propósito de una indicación del Ejecutivo[85] que en primer lugar alteraría el artículo cambiando su numeración al 11, pero además añadiría un nuevo literal z) al mismo. Respecto de los literales que ya fueron objeto de análisis previo, el literal b) que originalmente se refería a la dictación de disposiciones por parte de la Agencia fue convenido de la siguiente forma:

"*Dictar los protocolos y estándares que señala el artículo 7; las instrucciones generales y particulares, de carácter obligatorio, para las instituciones tanto públicas como privadas*

[84] CHILE. Ley N.º 19.880, *Establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado*. Diario Oficial de la República de Chile, Santiago de Chile, 29 de Mayo de 2003. Disponible en: https://bcn.cl/2ips6

[85] SGP. *Oficio N° 184-371*. 11 de octubre de 2023b. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32513&prmTIPO=OFICIOPLEY

obligadas por la presente ley; y las demás disposiciones necesarias para la aplicación y el cumplimiento de esta ley y sus reglamentos[86]"

Anteriormente, la crítica realizada contra esta disposición tenía relación con la referencia a instituciones públicas como privadas, cuando aún no existía tanta claridad respecto de la forma de calificación tanto de servicio esencial como de operadores de importancia vital. Ello fue subsanado con la modificación del artículo 4° tendiente a esclarecer precisamente dicha duda, de ahí que la nueva formulación de este literal opte por decir "instituciones públicas como privadas obligadas por la presente ley". Por su parte, la nueva configuración se refiere a la dictación de "protocolos y estándares", lo cual parece ser más adecuado considerando el ámbito técnico en el que se desarrolla la ciberseguridad.

Siguiendo con los literales ya analizados tenemos la letra e) relativo a la coordinación y la comunicación de incidentes entre el CSIRT nacional y la ANCI. Se trata de un literal que se mantuvo con la nueva indicación y que se aprobó de dicha forma. Sin embargo, se trata de una disposición que vinculábamos al artículo 7° que contenía el deber de reportar y que luego de su segundo trámite constitucional paso a ser el artículo 9°. Pues bien, este último ya no exige el deber de reportar independiente de si las instituciones publicas o privadas sean o no operadores de servicios esenciales, la modificación del mismo hizo que exista una remisión al artículo 4°, de manera que el deber se extiende a "todas" las instituciones públicas o privadas que en dicho artículo se señale. Aunado a ello, hay una mejoría en el esquema de reporte apreciable en los plazos y responsabilidades de las instituciones aludidas, si embargo, el plazo inicial en el cual se debe efectuar el reporte de un incidente de ciberseguridad se mantiene en las 3 horas[87].

Respecto del literal g), este sufrió una modificación mediante las indicaciones del Ejecutivo, quedando de la siguiente forma:[88]

"*Calificar, mediante resolución fundada y en la forma prevista en los artículos 4, 5 y 6 de esta ley, a los servicios esenciales y a los operadores de importancia vital*".

Se trata de una nueva formulación compatible con lo establecido en los nuevos artículos 4°, 5° y 6°. De esta forma, con las modificaciones de los expertos realizadas al artículo 4°, se logró dar mayor claridad y certeza jurídica a cuáles serán los servicios calificados de

[86] Ibid., pp. 1.
[87] CSC, 2023b, op. cit, pp. 77-82.
[88] SGP, 2023b, op. cit, pp. 2.

esenciales u operadores de importancia vital en función de los criterios establecidos en el nuevo artículo 5° y también con los respectivos recursos que podrían tener los regulados en contra de dicha calificación mediante el nuevo artículo 6°, cuestión que como ya comentábamos fue objeto de inquietud por parte de los parlamentarios en más de una sesión.

Un literal que también fue objeto de análisis previo en este documento fue el j) referido a los requerimientos que podría hacer la Agencia tanto a organismos del Estado como privados respecto de antecedentes u información para el cumplimiento de sus fines, ello incluso suponía el acceso a redes o sistemas informáticos de ser necesario. Producto de la falta de consenso al respecto, sobre todo en lo que guarda relación con la protección de los datos personales y la necesidad de requerir una autorización judicial para acceder a dicha información[89], el Ejecutivo propuso dos indicaciones al este literal, siendo la segunda de ellas la que finalmente fue aprobada por la comisión y que reviste el siguiente tenor[90]:

"*j) Requerir a los organismos de la Administración del Estado y a las instituciones privadas señaladas en el artículo 4 de la presente ley acceso a la información estrictamente necesaria para prevenir la ocurrencia de incidentes de ciberseguridad o para gestionar uno que ya hubiera ocurrido. Para lo anterior, podrá requerir la entrega del registro de actividades de las redes y sistemas informáticos que permitan comprender detalles de los incidentes de ciberseguridad que puedan haber ocurrido.*

Para el ejercicio de esta atribución, la instrucción siempre tendrá carácter particular, debiendo especificarse la información solicitada y fundarse debidamente. Cuando la información referida en el inciso anterior pudiera incluir datos personales estos deberán ser anonimizados, siempre que ello sea posible sin entorpecer la gestión de incidentes. En cualquier caso, los datos personales sólo podrán ser tratados dando estricto cumplimiento a lo dispuesto en la ley 19.628, y en particular, al principio de finalidad, sin perjuicio de lo que define la presente ley y sus reglamentos.

Con todo, para efectos de lo dispuesto en esta ley, no se considerará que la dirección IP sea un dato personal.".

[89] CSC, 2023b, op. cit, pp. 96-98.
[90] SGP. *Oficio N° 198-371*. 25 de octubre de 2023c. pp. 2. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32601&prmTIPO=OFICIOPLEY

Las modificaciones en torno a este literal se aprecian sobre todo en el hecho de que el señalamiento a organismos de la administración del Estado e instituciones públicas guarda relación con lo dispuesto en el renovado artículo 4°, destacando la necesidad de que el requerimiento al que se refiere sea debidamente fundado por la Agencia.

CAPÍTULO TERCERO: LA COMISIÓN PARA EL MERCADO FINANCIERO

3.1 ORÍGENES

La regulación del ámbito financiero en nuestro país ha sido algo dispersa desde mediados del siglo XIX. En ese sentido, uno de los hitos más relevantes al respecto recién vino a ocurrir en 1925 con la promulgación del DL N.º 559, que establecía la Ley General de Bancos. Posteriormente, entre 1927 y 1928 la Ley N.º 4.228 creó la Superintendencia de Compañías de Seguros, mientras que la Ley N.º 4.404 fundó la Inspección General de Sociedades Anónimas y Operaciones Bursátiles[91].

La evolución histórica en la materia continua en 1931, cuando el DFL N.º 251 fusiona los dos entes previamente mencionados, dando origen a la Superintendencia de Sociedades Anónimas, Compañías de Seguros y Bolsas de Comercio. En 1975, por su parte, el DL N.º 1.097 crea la Superintendencia de Bancos e Instituciones Financieras (SBIF)[92].

Ya en 1980, el DL N.º 3.538 crea a la Superintendencia de Valores y Seguros (SVS) la cual se erige como continuadora legal de la de la Superintendencia de Compañías de Seguros, Sociedades Anónimas y Bolsas de Comercio de 1931. Bastaría el paso de casi 30 años para que en 2017 la ley N.º 21.000 crease a la Comisión para el Mercado Financiero (CMF) que reemplazaría a la vigente SVS, y más tarde en 2019 mediante la ley N.º 21.130 que moderniza la legislación bancaria, absorbería a la SBIF, convirtiéndose así en el principal ente encargado del mundo financiero[93].

La CMF (o también “la Comisión”) se caracteriza por ser un servicio público descentralizado, de carácter técnico, dotado de personalidad jurídica y patrimonio propio, que se relaciona con el Presidente de la República a través del Ministerio de Hacienda. Dada su importancia en el sector financiero, sus objetivos están precisamente orientados a velar por el correcto funcionamiento, desarrollo y estabilidad del mercado financiero, facilitando la participación de los agentes de mercado y promoviendo el cuidado de la fe pública. Su labor no termina allí, sino que además se extiende a velar que los regulados cumplan con las leyes,

[91] COMISIÓN PARA EL MERCADO FINANCIERO (CMF). *Reseña histórica*. [En línea], s/f, Disponible en: https://www.cmfchile.cl/portal/principal/613/w3-article-23902.html
[92] Ibid.
[93] Ibid.

reglamentos, estatutos y cualquier otra normativa que los rija desde que estos inicien sus actividades y hasta que terminen por vía de la liquidación[94].

A la Comisión le compete lo establecido en su propia ley, así como también lo establecido en la ley N.º 18.575 relativa a las Bases Generales de la Administración del Estado, la ley Nº 19.880 sobre Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado y la Ley N.º 20.880 sobre Probidad en la Función Pública y Prevención de los Conflictos de Intereses. Resulta destacable que, tratándose del examen de las cuentas de sus gastos, puede quedar sometida a la fiscalización de la Contraloría General de la República[95].

Estos objetivos que se le han impuesto a la CMF se aplican en torno a una gran cantidad de regulados establecidos en el artículo 3° de su ley, esto en parte porque hemos apreciado que la Comisión ha absorbido a otras entidades especializadas, acaparando en ese sentido a los regulados que estas vigilaban, transformándose en un ente con alta especialización en el área financiera.

3.2 ATRIBUCIONES DE LA COMISIÓN PARA EL MERCADO FINANCIERO

La Comisión para el cumplimiento de sus objetivos está provista de diversas atribuciones, las cuales se establecen en el artículo 5° de su ley. Dicho artículo posee un total de treinta y cinco atribuciones, más una trigésima sexta que deja abierta la posibilidad de que otras leyes le confieran expresamente alguna determinada facultad. Para efectos de cumplir con los objetivos de este ensayo se analizarán aquellas pertinentes, teniendo esa cualidad aquellas que puedan presentar discrepancias con las ya comentadas de la ANCI en el capítulo anterior.

En ese sentido, una primera observación se puede realizar respecto a lo dispuesto en el artículo 5° numeral 1, que establece como facultad de la comisión lo siguiente:

"*Dictar las normas para la aplicación y cumplimiento de las leyes y reglamentos y, en general, dictar cualquier otra normativa que de conformidad con la ley le corresponda para la regulación del mercado financiero. De igual modo, corresponderá a la Comisión interpretar administrativamente las leyes, reglamentos y demás normas que rigen a las*

[94] CHILE, Ley N.º 21.000 *que crea la Comisión para el Mercado Financiero*. Diario Oficial de la República de Chile, Santiago de Chile, 27 de febrero de 2017. Artículo 1°. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1100517
[95] Ibid., Artículo 2°.

personas, entidades o actividades fiscalizadas, y podrá fijar normas, impartir instrucciones y dictar órdenes para su aplicación y cumplimiento. Estas potestades no podrán extenderse en ningún caso a las facultades normativas e interpretativas que le corresponden al Banco Central de Chile de conformidad con la ley, sin perjuicio de lo dispuesto en el artículo 82 de su ley orgánica constitucional"[96].

De la revisión de esta disposición es posible percatarse de una similitud con lo ya mencionado sobre el artículo 9° letra b) del proyecto despachado del Senado, es decir, una facultad de dictación de normas. Si bien se establece la diferencia de que en este caso debe tratarse de normas que tengan relación con el mundo financiero, mientras que el proyecto está orientado a los incidentes de ciberseguridad, no debemos olvidar que en el mundo financiero actual existe una importante dependencia de las redes y sistemas informáticos. En ese sentido, la ciberseguridad no es completamente ajena al ámbito financiero.

La prueba de esta labor normativa de la CMF en torno a la ciberseguridad se encuentra principalmente en la "Recopilación Actualizada de Normas" (RAN) contenidas en la circular N.º 2.409, incluyendo el capítulo 20-10 incorporado por la circular N.º 2.261 de julio de 2020, además de la "Norma de Carácter General" (NGC) N.º 454 ejecutada en mayo de 2021 por la resolución exenta N.º 2.606, ambas impartidas principalmente en virtud de la facultad que establece el numeral en comento.

La RAN alude a la ciberseguridad de forma concreta en el capítulo 20-10, sin embargo, ya capítulos previos entendían la relevancia de contar con sistemas o procedimientos adecuados en torno la seguridad en, por ejemplo, la transferencia electrónica de información y fondos[97]. Por su parte, el capítulo 20-10 vigente desde diciembre de 2020 fue precursor respecto de la materia, determinando lineamientos mínimos que deben cumplir las entidades reguladas en torno a la gestión de la seguridad de la información y la ciberseguridad[98], se incluyen además diversos tópicos como el proceso de gestión de riesgos, protección de los activos críticos y detección de amenazas, respuestas ante incidentes, entre otros. Curiosamente, incluye también un anexo con definiciones

[96] Ibid., Artículo 5° N.º 1.
[97] CHILE. Circular N.º 2.409. 13 de diciembre de 1988. Capítulo 1-7. Disponible en: https://bcn.cl/3a6sn
[98] Ibid., Capítulo 20-10, punto 1.

relevantes, las cuales son tratadas de forma similar en el proyecto, tales como: ciberespacio, incidente de seguridad, ciberincidentes, etc.

Por otro lado, la Norma de Carácter General (NGC) N.º 454 es el resultado de los esfuerzos de la Comisión por fortalecer el marco de supervisión para el mercado de seguros en nuestro país. En la búsqueda de dicho fortalecimiento, la CMF decidió emitir dicha normativa, cuyo objetivo es establecer los principios para mejores prácticas en un sistema de gestión del riesgo operacional y ciberseguridad[99]. En ese sentido, el objetivo principal de esta norma es, precisamente, establecer los principios y conceptos que rigen la gestión de riesgo operacional y la ciberseguridad, pero además de ello tiene otros objetivos como el establecimiento de una autoevaluación para las instituciones que sirva como diagnóstico sobre el cumplimiento de los principios y el establecimiento del deber de los regulados de reportar en caso de un incidente operacional o de ciberseguridad. En definitiva, se trata de objetivos que buscan fortalecer la supervisión de la comisión respecto de sus regulados[100].

De lo mencionado podemos determinar que la comisión posee facultades normativas, las cuales abarcan incluso materias de ciberseguridad. Por otro lado, aprovechando la mención de la NGC N.º 454, en el capítulo anterior se examinó la letra e) del artículo 9° del proyecto relativo a los tiempos de comunicación de los incidentes, así como también la mención al artículo 7° que se refiere al deber de reportar. Pues bien, como ya se indicó, uno de los objetivos la norma N.º 454 es el establecimiento del deber de reportar por parte de los regulados, lo que podría suponer una discrepancia entre estas normas.

En este contexto, la NGC, al referirse a la comunicación de incidentes operacionales, establece un deber de las compañías de seguro de reportar a la Comisión cuando tales incidentes sean de tal magnitud que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus asegurados, calidad de los servicios o la imagen de la institución, disponiendo de un tiempo máximo de 30 minutos para reportar desde que se ha tenido conocimiento del incidente[101]. Lo dispuesto por la norma guarda concordancia con lo previamente establecido por la RAN respecto de las entidades bancarias[102].

---

[99] CMF. *Informe normativo: Gestión de Riesgo Operacional y Ciberseguridad*. Mayo de 2021, pp. 4. Disponible en: https://bit.ly/3R9QKc4
[100] Ibid., pp. 5.
[101] CHILE. Norma de Carácter General N.º 454. 18 de mayo de 2021, pp. 36. Disponible en: https://www.cmfchile.cl/normativa/ncg_454_2021.pdf
[102] CHILE, 1988, op. cit., Capítulo 20-8.

La discrepancia que se puede apreciar está dada en ese sentido por a quién deberá reportarse en caso de un incidente de ciberseguridad, ¿A las entidades establecidas por el proyecto o al regulador financiero? ¿En un lapso de 30 minutos o de 3 horas? Teniendo en cuenta lo adelantada que ha sido la Comisión en la materia, podemos decir que tiene las capacidades necesarias para ser el ente que reciba los reportes y cree las normas que determine necesarias para el ámbito financiero, incluso tratándose de ciberseguridad, toda vez que esta es una cuestión que sin dudas puede continuar evolucionando. Ya en la discusión parlamentaria se advertían estas características por parte de la comisionada Bernardita Piedrabuena, quién, si bien rescataba la relevancia del proyecto y la creación de la ANCI, expresaba sus reparos de lo que la nueva normativa implicaría considerando el carácter autónomo de la CMF respecto de sus supervisados[103].

La modificación en el segundo trámite constitucional que alteró la numeración del proyecto haciendo que el artículo 9° letra b) sea el 11° letra b), no cambia el hecho de que se aprecia una duplicidad normativa, en este caso, relativa a la dictación de protocolos y estándares en materia de ciberseguridad. Por otra parte, en cuanto al artículo 9° letra e), actual 11° letra e), y en relación con el actual 9° sobre el deber de reportar las conclusiones son las mismas a las ya reseñadas, por cuanto la limitación temporal respecto del primer reporte se mantiene en las 3 horas.

Continuando con el estudio de las facultades que establece el artículo 5° de la Ley N.º 21.000, es pertinente referirse al numeral cuarto. En lo relevante para el análisis, dicho numeral establece la siguiente facultad de la CMF:

"*4. Examinar sin restricción alguna y por los medios que estime pertinentes todas las operaciones, bienes, libros, cuentas, archivos y documentos de las personas, entidades o actividades fiscalizadas o de sus matrices, filiales o coligadas, y requerir de ellas o de sus administradores, asesores o personal, los antecedentes y explicaciones que juzgue necesarios para obtener información acerca de su situación, sus recursos, de la forma en que se administran sus negocios e inversiones, de la actuación de sus personeros, del grado de seguridad y prudencia con que hayan invertido sus fondos, cuando corresponda y, en general, de cualquier otro punto que convenga esclarecer para efectos de determinar el cumplimiento de la normativa aplicable por parte de la entidad fiscalizada*…"[104]

[103] CDNSPU, 2023. op. cit. pp. 137.
[104] CHILE, 2017. op. cit., Artículo 5° N.º 4 inciso 1.

Este numeral se asemeja a lo establecido en el literal j) del artículo 9° redactado en el primer trámite constitucional, por cuanto la normativa de la CMF añade la posibilidad de que esta solicite la entrega de cualquier documento, libro o antecedente que sea necesario para fines de fiscalización o estadística[105]. Nuevamente, se observa una diferencia con el proyecto al señalar que los fines con los que se hace esta solicitud son aquellos que persigue la ANCI, es decir, fines relacionados principalmente con la ciberseguridad. Sin embargo, ya advertíamos que, aunque no esté expresamente indicado en la ley que crea la CMF, es indudable su competencia en materia de seguridad de datos y sistemas informáticos.

En ese sentido, esta facultad que establece el numeral cuarto de examinar o realizar requerimientos en contra de los regulados está fundada en que dicha exigencia se realiza con el fin de determinar si se ha cumplido o no con normativa aplicable, entre las cuales tenemos aquellas que se refieren a la ciberseguridad. En ese sentido, si una aseguradora sufriera un incidente de ciberseguridad, la comisión en virtud de la NGC N.º 454 podría requerir documentos de la entidad, por ejemplo, para determinar si esta cumplió con la obligación de reportar y si lo hizo dentro del plazo que la normativa establece.

Las conclusiones sobre esta discrepancia son las mismas tratándose de la formulación fruto de la discusión en la Comisión de Seguridad Ciudadana perteneciente a la Honorable Cámara de Diputados. Ello por cuanto el actual artículo 11° j) sigue permitiendo una facultad de requerimiento respecto de sus regulados.

Como hemos apreciado, la CMF en tanto ente autónomo posee cierta trayectoria en torno a la seguridad en las redes y sistemas informáticos, incluso siendo capaz de adecuarse a la rápida evolución que tiene esta materia. Un ejemplo actual de ello son los esfuerzos de la Comisión por implementar la reciente ley N.º 21.551 dedicada a establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos que realicen los proveedores regidos por ella[106], pues es justamente el empleo de tales medios tecnológicos lo que supone un necesario análisis a la ciberseguridad que debe respaldarla.

[105] Ibid., Artículo 5° N° 4 inciso 3.
[106] CHILE. Ley N.º 21.521 *Que Promueve la Competencia e Inclusión Financiera a través de la Innovación y Tecnología en la Prestación de Servicios Financieros* (Ley FINTEC). Diario Oficial de la República de Chile, Santiago, Chile, 4 de enero de 2023. Artículo 1° inciso 1. Disponible en: https://bcn.cl/3b2f5

El proyecto de ley despachado por el Senado, y fruto de las de las discusiones en comisiones especializadas dentro del mismo, buscó resolver las discrepancias que ya hemos señalado y en consecuencia fueron redactados los artículos 21° y 22°, el primero de ellos encargado de establecer a los CSIRT sectoriales, señalando a la CMF como un ente fiscalizador de un futuro CSIRT financiero, mientras que el artículo 22° que establece las facultades especiales de los CSIRT sectoriales, disponiendo en su inciso final lo siguiente:

"*Tratándose de sus instituciones fiscalizadas, la Comisión para el Mercado Financiero podrá establecer las normas de carácter general y técnicas sobre ciberseguridad sin necesidad de solicitar la aprobación de la Agencia, siempre y cuando tengan un alcance distinto a las normas dictadas por ella. En caso de que la Comisión para el Mercado Financiero emita normativa que regule elementos contenidos en normas, protocolos o instrucciones generales dictados por la Agencia, deberá informarle previamente, remitiendo la norma, protocolo o instrucción, con una anticipación de, al menos, treinta días hábiles a su emisión por parte de la Comisión para el Mercado Financiero*".[107]

Con lo anterior, se creía solucionar la duplicidad normativa que pudiere producirse entre la ANCI y la CMF en el desempeño de sus facultades normativas manteniendo esta última cierta autonomía, pues se le exime de solicitar la aprobación de la agencia toda vez que sus normas tengan un alcance distinto, y además permitiéndole actuar como fiscalizador del CSIRT de su ámbito financiero.

Por otra parte, posterior al debate ante la Comisión de Seguridad Ciudadana, y en función del principio de coordinación que se estableció en esta instancia, los artículos 21° y 22° ya mencionados fueron suprimidos, esto debido a que el título IV aludido con anterioridad suprime por completo la mención a los CSIRT sectoriales, y en consecuencia el primer artículo de dicho título, es decir, el artículo 25°[108], se refiere a la coordinación regulatoria. Esta sería la solución a la que arribó la CSC con el propósito de prevenir un conflicto normativo entre ANCI y CMF. Dicho artículo es una norma espejo del artículo 37° bis de la Ley 19.880 con sus modificaciones correspondientes[109], estableciendo la necesidad de que la Agencia solicite un informe a la entidad sectorial con el propósito de prevenir posibles conflictos normativos, garantizando así la coordinación regulatoria.

[107] CSC, 2023a, op. cit., pp. 42. Artículo 22.
[108] CSC, 2023b, op. cit., pp. 213.
[109] Ibid., pp. 71.

Asimismo, el artículo 26°[110] hace referencia a la normativa sectorial y en su inciso tercero fija la prevalencia de las normas dictadas de la autoridad sectorial por sobre la de la Agencia cuando dichas normas sean a lo menos equivalentes a aquellas previstas por la ANCI.

Respecto de este segundo trámite constitucional resulta destacable la eliminación de la referencia a CSIRT sectoriales por el vocablo autoridad sectorial. De esta manera, creemos que es una forma de aprovechar la institucionalidad existente manteniendo a la CMF en el cumplimiento de facultades relacionadas con la ciberseguridad.

[110] Ibid., pp. 213.

CAPÍTULO CUARTO: DERECHO COMPARADO.

Expuestas las pretensiones del proyecto, sobre todo en términos de la creación de una agencia especializada en materia de ciberseguridad, resulta pertinente examinar como se han comportado países como España y Reino Unido, los cuales precisamente han servido de inspiración para el proyecto nacional[111].

4.1 CONTEXTO ESPAÑOL EN TORNO A LA CIBERSEGURIDAD

A pesar de que en España persiste una disparidad entre aquellos que las utilizan y aquellos que no utilizan las tecnologías de la información y comunicación, situación que puede ser atribuida a una serie de factores, el empleo de dichas tecnologías en los hogares ha experimentado un aumento en los últimos años. De esta forma, para el año 2022, los datos que entrega el Instituto Nacional de Estadísticas (INE) español acerca del uso del internet dan cuenta de que el 94,5% de la población entre 16 y 74 años utiliza el internet con cierta regularidad, lo que equivale a más de 33 millones de usuarios[112]. Esto supone, como hemos visto a lo largo de este documento, una mayor cantidad de personas expuestos a los riesgos que conlleva el uso de las TICs y el internet en general.

En ese contexto, el Estado español se ha visto obligado, al igual que ya apreciábamos en nuestro país, en la necesidad de asumir nuevos retos para los instrumentos del Estado, esto en parte porque la lucha contra el cibercrimen requiere de herramientas y técnicas distintas a las tradicionales, lo que ha significado el desarrollo de o bien nuevos organismos o secciones dentro de los ya existentes para precisamente adaptarse a las incipientes amenazas en contra de la ciberseguridad. Por otro lado, la propia definición de la materia supone un reto, esto al no existir un consenso acerca de los múltiples conceptos que se desenvuelven en esa disciplina, lo cual resulta razonable advirtiendo que se trata de un contexto en constante evolución, pero que por ese mismo detalle puede llevar a confusiones jurídicas[113].

Por su parte, la capacidad de responder ante las amenazas mencionadas, en la práctica, se ve coartada por el hecho de que los ciberincidentes no son reportados a las autoridades

---

[111] OLMOS, Renato, 2023, op. cit.
[112] INE. *Población que usa Internet (en los últimos tres meses). Tipo de actividades realizadas por Internet*. [En línea] 2022, Disponible en: https://bit.ly/45DQWFR
[113] DEL REAL, Cristina. *Panorama institucional de la gobernanza de la ciberseguridad en España*. Revista de Estudios Jurídicos y Criminológicos, N.º 6, Universidad de Cádiz. 2022, pp. 17. Disponible en: https://doi.org/10.25267/REJUCRIM.2022.i6.03

competentes, siendo solo una porción reducida de estos los que efectivamente son denunciados. Sin perjuicio de ello, lo cual se funda en diversas causas, España, ha seguido un modelo de seguridad plural según el cual conviven diversas instituciones estatales y prácticas de ciberseguridad[114]. No obstante lo anterior, las estadísticas del observatorio español de delitos informáticos dan cuenta de un aumento de los ciberdelitos que se ha mantenido constante desde 2011[115].

En cualquier caso, si queremos examinar la situación de la gobernanza española en torno a la ciberseguridad, necesariamente debemos referirnos a las normativas europeas. Ya mencionábamos con anterioridad en este ensayo el Convenio de Budapest promulgado por nuestro país en 2017, el cual ya poseía una larga data, toda vez que su origen se dio en Consejo Europeo en el año 2001. En el caso español, la ratificación del mismo se produjo en el año 2010.

Otra normativa europea relevante que ha influido en el Estado español es la Directiva (UE) 2016/1148 (conocida popularmente como NIS 1) que tenía por finalidad incentivar a los Estados miembros a adoptar medidas para reforzar la seguridad de las redes y sistemas de información. Con el propósito de lograr ese cometido dispuso de diversos objetivos como: i) establecer la obligación para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; ii) crear un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros; iii) crear una red de equipos de respuesta a incidentes de seguridad informática (*computer security incident response teams* o CSIRT); iv) establecer requisitos en materia de seguridad y notificación para los operadores de servicios esenciales, así como también para los proveedores de servicios digitales; v) establecer obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas con la seguridad de las redes y sistemas de información[116].

---

[114] Ibid., pp. 18-20.
[115] OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS (OEDI). *Estadísticas*. [En línea] 2021, Disponible en: https://oedi.es/estadisticas/
[116] UNIÓN EUROPEA (UE). *Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea, 10 de julio de 2016. pp. 11, Artículo 1. Disponible en: http://data.europa.eu/eli/dir/2016/1148/oj

La mencionada directiva fue traspuesta por el Estado español en 2018[117], sin embargo, ya en 2020 se comenzó a discutir en la Unión una nueva directiva conocida como NIS 2, que entró en vigencia desde enero de 2023[118], y que dispone de un periodo de 21 meses para ser incorporada a la legislación de los países miembros. Esta última situación denota lo rápido que puede ser la evolución de esta materia y la necesidad de adecuarse a dicha evolución, como ya se ha mencionado tantas veces a lo largo de este ensayo.

Por otro lado, en relación con las influencias del Estado español no puede no mencionarse a ENISA, pues se trata de una agencia que ha buscado promover el establecimiento de un ecosistema de ciberseguridad europeo a través de actuaciones de *soft law* que tienen por objetivo armonización de las políticas de ciberseguridad entre los Estados miembros. Además de esta entidad, el contexto europeo contiene a la "Agencia Europea de Defensa" (EDA) que trabaja para desarrollar la política de ciberdefensa europea, el "Centro Europeo de Cibercrimen" (EC3) que actúa como unidad de apoyo técnico a operaciones de lucha contra el cibercrimen en Europa e incluso en 2021 se añadió a esta lista el "Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad"[119] cuya finalidad es contribuir a aumentar las capacidades y la competitividad de Europa en investigación, tecnología y desarrollo industrial de la ciberseguridad[120].

En el ámbito nacional español una norma relevante en torno a la materia es la ley N.º 8 de 2011 [121] que se refiere principalmente a las medidas para la protección de las infraestructuras críticas. Dicha ley, indica que organismos o agentes forman parte del "Sistema de Protección de Infraestructuras Críticas", entre ellos se encuentra el "Centro Nacional para la Protección de las Infraestructuras Críticas", el cual, creado en 2007, actúa como responsable del impulso, coordinación y supervisión de todas las políticas y

[117] ESPAÑA. Real Decreto-Ley 12/2018 *de seguridad de las redes y sistemas de información*, 7 de septiembre de 2018. https://www.boe.es/eli/es/rdl/2018/09/07/12
[118] UNIÓN EUROPEA (UE). *Directiva 2022/2555 del parlamento europeo y del consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la unión, por la que se modifican el reglamento (UE) Nº 910/2014 y la directiva (UE) 2018/1972 y por la que se deroga la directiva (UE) 2016/1148 (directiva SRI 2)*. Diario Oficial de la Unión Europea, 27 de diciembre de 2022. Disponible en: http://data.europa.eu/eli/dir/2022/2555/oj
[119] UNION EUROPEA (UE). *Reglamento 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación*. Diario Oficial de la Unión Europea, 8 de Junio de 2021 Disponible en: http://data.europa.eu/eli/reg/2021/887/oj
[120] DEL REAL, Cristina. 2022, op cit., pp. 28.
[121] ESPAÑA. Ley 8/2011 *por la que se establecen medidas para la protección de las infraestructuras críticas*. 28 de abril de 2011. Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8/con

actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior[122].

Continuando con la normativa española, cobran relevancia las políticas o estrategias nacionales de seguridad o ciberseguridad. Precisamente la primera estrategia de ciberseguridad a la que podemos aludir es a la publicada en 2013 por parte del gobierno español. Esta estrategia fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone la vulnerabilidad del ciberespacio, además, diseñaba el modelo de gobernanza para la ciberseguridad nacional[123]. Descartando la estrategia anterior, se publica una nueva táctica de seguridad nacional en 2017, que, aunque no está enfocada en la ciberseguridad, incluye una multitud de referencias a conceptos relacionados con la misma, así como también estableciendo objetivos y lineamientos en torno a dicha temática[124]. Por último, la estrategia que se encuentra en actual vigencia data desde 2019, en este caso si se trata de una estrategia netamente dedicada a la ciberseguridad, en la que se desarrollan los objetivos y lineamientos ya establecidos en la anterior[125],

Analizar la gobernanza española en plenitud es una tarea compleja considerando que ya mencionamos la existencia de una dispersión en ese sentido, sin embargo, podemos establecer una diferenciación entre órganos políticos, técnicos u operativos. Al respecto, los órganos políticos son aquellos que están compuestos por cargos electos y cuya función principal es la elaboración de políticas, planes y estrategias. Por su parte, los órganos técnicos serían aquellos compuestos por personal especialista en alguna materia y cuyo objetivo principal sería asesorar a los ya mencionados órganos políticos. Por último, los órganos operativos serían aquellos que ejecutan de manera instrumental los planes, programas y políticas, y prestan los servicios conforme a las políticas diseñadas desde "arriba"[126].

En función de esa distinción y para los efectos de este documento, nos enfocaremos en un ente operativo como lo es el Instituto Nacional de Ciberseguridad (INCIBE), el cual forma

[122] GAYOSO, Víctor, HERNÁNDEZ, Luis y ARROYO, David. 2020, op. cit., pp. 39.
[123] ESPAÑA. DEPARTAMENTO DE SEGURIDAD NACIONAL. *Estrategia de ciberseguridad nacional*. 2013. Disponible en: https://bit.ly/488ZlCS
[124] ESPAÑA. Real Decreto 1008/2017 *por el que se aprueba la Estrategia de Seguridad Nacional 2017*. 21 de diciembre de 2017. Disponible en: https://www.boe.es/eli/es/rd/2017/12/01/1008/con
[125] ESPAÑA. Orden PCI/487/2019 *por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional*. 26 de abril de 2019. Disponible en: https://www.boe.es/eli/es/o/2019/04/26/pci487/con
[126] DEL REAL, Cristina. 2022, op cit., pp. 30.

parte del Esquema Nacional de Seguridad (ENS)[127], que además es dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, órgano político que a su vez es dependiente del Ministerio de Asuntos Económicos y Transformación Digital, otro ente político. Igualmente, y aunque no se le considera un órgano operativo, corresponde referirse al Consejo Nacional de Ciberseguridad (CNC), toda vez que este es el principal organismo de cooperación política en la materia. Precisamente, el CNC es el encargado de coordinar la estrategia de ciberseguridad, además de otras labores, en virtud del artículo 21° de la Ley 36/2015, y en la práctica en el cumplimiento de dicho mandato ha aportado a la formulación de las estrategias nacionales de ciberseguridad de 2013 y 2019.

Pues bien, el INCIBE no se ha denominado siempre como lo hace actualmente, sus orígenes se remontan al año 2006 con la fundación del instituto nacional de tecnologías de la información (INTECO) como parte de un plan de gobierno dedicado a promover el uso de las TICs. Tendría que llegar el año 2013 para que recién INTECO cambiara su enfoque y se convirtiera en el actual INCIBE, principal organismo dentro de España encargado de la concienciación en ciberseguridad a empresas y ciudadanos[128]. Se trata de un órgano operativo que se dedica a mejorar el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación, los profesionales, las empresas y, especialmente, los sectores estratégicos[129].

En tal sentido, podríamos decir que el homólogo español de la Agencia Nacional de Ciberseguridad que se pretende crear en nuestro país es el INCIBE, el cual dispone también de variadas funciones, tales como las siguientes[130]:

- Mejorar la ciberseguridad y la confianza digital de ciudadanos, menores y empresas privadas de España.
- Proteger y defender a los ciudadanos, menores y empresas privadas de España.
- Potenciar la industria española de ciberseguridad.
- Impulsar la I+D+i española en ciberseguridad.
- Identificar, generar, atraer y desarrollar profesionales del sector de ciberseguridad.

[127] ESPAÑA. Real Decreto 311/2022 *por el que se regula el Esquema Nacional de Seguridad*. 3 de mayo de 2022. Disponible en: https://www.boe.es/eli/es/rd/2022/05/03/311/con
[128] DEL REAL, Cristina. 2022. op. cit., pp. 34.
[129] GAYOSO, Víctor, HERNÁNDEZ, Luis y ARROYO, David. 2020, op. cit., pp. 39.
[130] INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Qué es INCIBE*. [En línea] s/f, Disponible en: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe

4.1.1 SITUACIÓN DEL REGULADOR FINANCIERO EN ESPAÑA.

La Comisión Nacional del Mercado de Valores (CNMV), creada por la ley 24/1988, es el organismo responsable de la supervisión e inspección de los mercados de valores españoles y de las actividades de quienes participan en ellos[131]. Tiene como función principal velar por la transparencia de los mercados de valores españoles, asegurando una formación de precios adecuada, encargándose a la vez de proteger los intereses de los inversores[132].

Con algunas de las características mencionadas se asemejaría a la labor que cumple la CMF en nuestro país, sin embargo, a diferencia de esta última, no posee normativa dedicada especialmente a la ciberseguridad en su esfera de competencias. Sin embargo, ello no quiere decir que esté completamente desligada de la materia, en ese aspecto, entiende los riesgos que conlleva la transformación tecnológica y concuerda con trabajar de forma colaborativa al respecto.

A este respecto, la CNMV ha participado en, por ejemplo, la elaboración del código de buen gobierno de la ciberseguridad originado en el seno del foro nacional de ciberseguridad. Por ello, aunque la comisión no es la autora del mismo, lo ha difundido a través de su página web, buscando que este contribuya al conocimiento entre las cotizadas y entidades supervisadas.

Este código se funda en diversas fuentes, entre las cuales tenemos la propia política nacional de ciberseguridad española de 2019, algunas leyes nacionales (311/2022, 43/2021) e internacionales (NIS 2) con la finalidad de desarrollar un trabajo de recopilación de principios fundamentales en torno a la gobernanza de la ciberseguridad de los órganos de gobierno.

En este caso, podríamos concluir que no existe una deferencia marcada por el ente financiero en torno a la ciberseguridad, sin embargo, la experiencia española nos permite comprender que no debiese haber un solo ente todopoderoso que se dedique a ello. Ya lo pudimos apreciar en el apartado anterior, en el cual además solo aludimos a los entes que parecieran tener mayor relevancia, sin embargo, la realidad es que no solo se limitan a los

[131] COMISIÓN NACIONAL DEL MERCADO DE VALORES (CNMV). *Funciones*. [En línea] s/f, Disponible en: https://www.cnmv.es/portal/quees/Funciones/Funciones.aspx
[132] Ibid.

allí aludidos, es decir, existe un amplio abanico de instituciones españolas que contribuyen a la ciberseguridad actuando en armonía y permanente colaboración[133].

La crítica en ese sentido estaría dada en que España puede decidir no darle atribuciones en materia de ciberseguridad al ente financiero porque se entiende que detrás de este existe un respaldo compuesto por una gran cantidad de organismos que precisamente se dedican a ello, estamos hablando de una estructura u organización con la que nuestro país no cuenta actualmente debido a su desarrollo incipiente.

4.2 CONTEXTO DEL REINO UNIDO EN TORNO A LA CIBERSEGURIDAD

Similar a lo observado en España, en el Reino Unido también existe una alta tasa de penetración del internet en la población. En ese aspecto los datos indican que en un periodo que va desde 2007 a 2020, el porcentaje de individuos que se conectaron a internet por día pasó de estar cerca de 50% a un 94% en el último año estudiado[134].

Por otro lado, en torno al control del cibercrimen, y desde 2016, Reino Unido cuenta con el "*National Cyber Security Center*" (NCSC), una entidad que actúa como punto de contacto para pequeñas y medianas empresas (PYMEs), grandes organizaciones, agencias gubernamentales y el público en general. Asimismo, colabora estrechamente con otras entidades de orden, defensa, agencias de inteligencia y seguridad tanto del Reino Unido como a nivel internacional[135].

De forma más específica esta agencia se dedica a:

- Entender la ciberseguridad y promover el conocimiento de la misma en orientaciones prácticas que ponen a disposición de toda la población.
- Responde a los incidentes de ciberseguridad para reducir el daño que causan a las organizaciones y al Reino Unido en general.
- Utilizar la experiencia de la industria y el mundo académico para fomentar la ciberseguridad en el Reino Unido.

[133] DEL REAL, Cristina. 2022. op. cit., pp. 31.
[134] STATISTA. *Porcentaje de individuos que se conectó a Internet diariamente en el Reino Unido de 2007 a 2020*. [En línea] 2022, Disponible en: https://bit.ly/3Q7ZGhG
[135] NATIONAL CYBER SECURITY CENTER (NCSC). *What we do*. [En línea] s/f, Disponible en: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

- Reducir los riesgos para el Reino Unido protegiendo las redes de los sectores público y privado.

Respecto del primer punto indicado, la NCSC está constantemente emitiendo guías y orientación en torno a la materia, esto se evidencia en blogs, artículos, entre otros. Recientemente, emitieron un documento que contiene una revisión anual de su labor como agencia y el desarrollo que han logrado en 2023. Dicho documento se dedica a abordar diversas temáticas que pueden tener relación con la ciberseguridad, así como también casos de estudio que permiten comprender la importancia que tiene la misma.[136]

Por otro lado, la NCSC tiene un sistema propio de gestión de incidentes (*Incident Management*) que tiene por finalidad reducir el daño causado por incidentes de seguridad cibernética en el Reino Unido, se trata de un equipo encargado de clasificar los incidentes, definir la respuesta del NCSC así como otros organismos del gobierno y prestar apoyo directo a las organizaciones de víctimas, en cooperación con el proveedor de respuesta a incidentes de la propia víctima[137].

El marco regulatorio en torno a la ciberseguridad se asemeja a lo que sucede en España, existiendo normativa primaria y secundaria al respecto. Expresión de ello, y en relación con la ciberseguridad, es la directiva 2016/1148, la cual fue aplicada a nivel interno a través del Reglamento de Redes y Sistemas de 2018 (Network and Information Systems Regulations) y que, sin perjuicio de que el Reino Unido ya no pertenece a la UE, mantiene su vigor con las correspondientes modificaciones que ese último hecho supone[138].

Asimismo, recientemente el gobierno publicó la estrategia nacional de ciberseguridad con objetivos propuestos entre un periodo que va desde 2022 a 2030[139] la cual establece diversos pilares estratégicos como también propuestas de transformación en relación con la disciplina de la ciberseguridad.

[136] NCSC. *Annual review 2023*. [En línea] 14 de noviembre de 2023, Disponible en: https://www.ncsc.gov.uk/collection/annual-review-2023
[137] NCSC. *What we do*. Op. cit.
[138] CLARK, Adam. *Cybersecurity in the UK*. House of Commons Library. 22 de Junio de 2023. Disponible en: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf
[139] HM GOVERNEMENT. Government Cyber Security Strategy 2022-2030. 2022. Disponible en: https://bit.ly/3RfVqxb

4.2.1 SITUACIÓN DEL REGULADOR FINANCIERO EN REINO UNIDO.

La ley de servicios financieros de 2012 abolió la Financial Services Authority (FSA), de forma que al entrar en vigor en abril 2013 se establecieron dos nuevos entes encargados de regular el mundo financiero, estos son la Financial Conduct Authority (FCA) y la Prudential Regulation Authority (PRA).

En esa dirección, la FCA se dedica a garantizar el correcto funcionamiento de los mercados respecto de los individuos, las empresas y la economía en su conjunto, para ello regula, supervisa y establece estándares específicos para miles de empresas en el Reino Unido[140]. En años recientes y para cumplir con sus objetivos ha creado una estrategia enfocada en un periodo de 3 años, esto es, entre 2022 y 2025. Dicha estrategia se impone como objetivo minimizar el impacto de las interrupciones operativas, entre ellas la creciente amenaza que suponen los ciberataques, frente a los cuales han introducido nuevas normas y orientaciones para reforzar la resiliencia operativa[141].

La FCA es una entidad que demuestra interés en la ciberseguridad de sus regulados, ello se ve reflejado en diversos aspectos como la estrategia que ya mencionamos, pero entendiendo que las ciberamenazas representan un riesgo relevante para el mercado financiero, desde 2017, esta autoridad ha realizado reuniones con empresas del rubro para colaborar en grupos sobre ciberseguridad y resiliencia operativa. Estos grupos recibieron el nombre de “Grupos de Coordinación Cibernética” (*Cyber Coordination Groups*) y su finalidad es ayudar a las empresas a compartir conocimientos y debatir buenas prácticas para protegerse de las amenazas cibernéticas. A estas reuniones asistieron otros organismos del Estado, entre ellos la NCSC, demostrando así el compromiso que ha asumido la FCA en la materia[142].

Así como los artículos mencionados en los que la FCA toma una iniciativa propia en la materia, en la web de la FCA nos podemos encontrar con una gran biblioteca de información relativa a la ciberseguridad. Parte de estos artículos dan cuenta de una coordinación

[140] Financial Conduct Authority (FCA). *About the FCA*. [En línea] 19 de abril de 2016, Disponible en: https://www.fca.org.uk/about/what-we-do/the-fca

[141] FCA. *Our strategy 2022 to 2025*. pp. 24. [En línea] s/f, Disponible en: https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf#page=3

[142] FCA. *Insights from the 2020 Cyber Coordination Groups*. [En línea] 29 de abril de 2021, Disponible en: https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups-2020

existente entre esta autoridad y la agencia de ciberseguridad, agencia de la cual toman recomendaciones y las hacen llegar a sus regulados.

CONCLUSIONES

En virtud de lo dispuesto y analizado a lo largo de este documento, podemos notar que nuestro país ha tenido un avance relevante durante los últimos años en materias de digitalización, tecnología y ciberseguridad. En ese sentido, ha sido valioso e inspirador lo ejecutado por otros países en el contexto internacional debido al desarrollo que, a diferencia de nosotros, presentan en la materia.

La discusión relativa a robustecer nuestra infraestructura de la información ha permitido que nos sentemos a la mesa a analizar la necesidad de contar con una institucionalidad que permita hacer efectivo ese fortalecimiento deseado. Sin embargo, crear un ente de esas características no es sencillo, al contrario, ha supuesto una multiplicidad de controversias, controversias que necesitan ser resueltas de antemano a fin de evitar promulgar una ley que puede no ser capaz de satisfacer los objetivos que le dieron origen.

Respecto a este punto, hasta el segundo trámite constitucional del proyecto de ley analizado, podríamos decir que al menos en el papel la controversia entre las facultades normativas de la ANCI y la CMF han sido resueltas. Ello se debe a dos cuestiones, en primer lugar, se considera a la Comisión como una autoridad financiera mientras que con anterioridad se pretendía crear un CSIRT financiero lo que a nuestro criterio ponía en peligro la autonomía normativa desarrollada por necesidad en el ámbito de la ciberseguridad. La segunda dice relación con considerar a la CMF como una autoridad sectorial con la capacidad de dictar normas generales en el marco financiero las que prevalecerán siempre que tenga efectos equivalentes a la normativa dictada por la ANCI.

No obstante lo anterior, nos reservamos el derecho a ser escépticos con los resultados que tendrá esta solución en la práctica ya que requerirá de un esfuerzo conjunto de ambas entidades en el cumplimiento de los principios establecidos en el proyecto, con especial consideración el principio de coordinación. En otro orden de ideas, será interesante observar lo que pueda suceder en un futuro cuando la ANCI logre tal nivel de especialización que el aprovechamiento de la institucionalidad que supone la CMF deje de ser necesario en el ámbito de la ciberseguridad.

Ello no quiere decir que deba desecharse una idea como la que se está planteando, sobre todo considerando que el desarrollo internacional nos demuestra que poseer una Agencia Nacional de Ciberseguridad no deja de ser valioso, y nos mantendría como pioneros en la región al lograr un avance de esas características.

Pudimos observar que la experiencia comparada posee una mayor trayectoria y una institucionalidad mucho más robusta que le permite posicionar las funciones en torno a la ciberseguridad en más de solo una entidad. Sí, el proyecto mismo propone otras entidades además de aquellas con las que ya contamos buscando acercarse así a la experiencia comparada, sin embargo, el catálogo de atribuciones pareciera estar radicado en solo una de ellas.

En nuestro país, a través de este proyecto, estamos dando uno de los pasos más relevantes propuestos por la PNCS en 2017, por ello debemos ser cuidadosos de que el mismo no represente un intento fallido de lograr los objetivos que alguna vez nos planteamos y que tan necesarios son de lograr teniendo en cuenta el estado actual de la evolución del Internet y todas las tecnologías asociadas a él. Será pertinente, en ese caso, cuidarse de las disposiciones que sean demasiado amplias, de definir con exactitud ciertos conceptos que pueden inducir a errores cuando sea posible siquiera definirlos, regular adecuadamente las atribuciones que se encomendarán, propiciar un ambiente colaborativo entre los distintos entes que participarán en el mundo de la ciberseguridad, entre otras. Solo así podremos lograr resguardar la seguridad de los habitantes de nuestro país o prevenir las amenazas y riesgos que los pueden afectar en el ciberespacio.

BIBLIOGRAFÍA

ÁLVAREZ, Daniel. *Agenda legislativa sobre ciberseguridad en Chile*. Revista Chilena De Derecho Y Tecnología, 7(2), 1–3. 2018, pp. 3. Disponible en: https://doi.org/10.5354/0719-2584.2018.51992

ÁLVAREZ, Daniel. *Los desafíos de la ciberseguridad en Chile*. Revista Chilena De Derecho Y Tecnología, 6(2), 1–2. 2017. Disponible en: https://doi.org/10.5354/0719-2584.2017.48027

BRENNER, Susan. *La Convención sobre Cibercrimen del Consejo de Europa*. Revista Chilena de Derecho y Tecnología. 1 (1): pp. 221-238. 2012. Disponible en: https://doi.org/10.5354/0719-2584.2012.24030

CLARK, Adam. *Cybersecurity in the UK*. House of Commons Library. 22 de Junio de 2023. Disponible en: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf

CMF. *Informe normativo: Gestión de Riesgo Operacional y Ciberseguridad*. Mayo de 2021. Disponible en: https://bit.ly/3R9QKc4

COMISIÓN DE LAS COMUNIDADES EUROPEAS (CCE). *Hacia una política general de lucha contra la ciberdelincuencia*. 22 de mayo de 2007. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0267

COMISIÓN DE SEGURIDAD CIUDADANA (CSC). *Comparado Segundo Trámite Constitucional, sobre el Proyecto de Ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la* información (Boletín n°14.847-06*)*. 10 de mayo de 2023.

COMISIÓN DESAFÍOS DEL FUTURO, CIENCIA, TECNOLOGÍA E INNOVACIÓN (CDFCTE). *Construyendo la ciberseguridad en chile*. Ediciones Biblioteca del Congreso Nacional de Chile. 2023, pp. 17. Disponible en: https://bit.ly/46Re6t6

COMISIONES DE DEFENSA NACIONAL Y DE SEGURIDAD PÚBLICA, UNIDAS (CDNSPU). *Segundo informe recaído en el proyecto de ley, en primer trámite constitucional, que establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información (Boletín N° 14.847-06)*. 20 de Abril de 2023. Disponible en: https://bit.ly/3Tkk02F

COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD (CIC). *Política Nacional de Ciberseguridad*. 27 de abril de 2017. Disponible en: https://biblioteca.digital.gob.cl/handle/123456789/738.

CSC. *Informe de la comisión de seguridad ciudadana recaído en el proyecto de ley que establece una ley marco sobre ciberseguridad e infraestructura crítica de la información, boletín N.º 14.847-06*. 27 de noviembre de 2023b. Disponible en: https://bit.ly/3TmeaxI

DEL REAL, C. Panorama institucional de la gobernanza de la ciberseguridad en España. Revista de Estudios Jurídicos y Criminológicos, n.º 6, Universidad de Cádiz, 2022. Disponible en: https://doi.org/10.25267/REJUCRIM.2022.i6.03

GAYOSO, Víctor, HERNÁNDEZ, Luis y ARROYO, David. *Ciberseguridad*. CSIC, 2020. Disponible en: https://www.digitaliapublishing.com/a/80863/ciberseguridad

HM GOVERNEMENT. *Government Cyber Security Strategy 2022-2030*. 2022. Disponible en: https://bit.ly/3RfVqxb

KAUR, Shubhdeep y RANDHAWA, Sukhchandan. *Dark Web: A Web of Crimes*. Wireless Personal Communications 112, 2131–2158. 2020. Disponible en: https://doi.org/10.1007/s11277-020-07143-2

LARA, Juan, MARTÍNEZ, Manuel y VIOLLIER, Pablo. *Hacia una regulación de los delitos informáticos basada en la evidencia*. Revista Chilena De Derecho Y Tecnología, 3(1). 2014. Disponible en: https://doi.org/10.5354/0719-2584.2014.32222

LEMOS, André. *CIBER-REBELDES*. 2023. Disponible en: https://www.researchgate.net/publication/265577731_CIBER-REBELDES

LÓPEZ, Manel. *Internet de las Cosas*. Rama Editorial. 2019. Disponible en: https://www.digitaliapublishing.com/a/110136/internet-de-las-cosas

MOSCOSO, Romina. *La Ley 19.223 en general y el delito de hacking en particular*. Revista Chilena de Derecho y Tecnología, 3(1). 2014. Disponible en: https://doi.org/10.5354/0719-2584.2014.32220

SECRETARIA GENERAL DE LA PRESIDENCIA (SGP). *Oficio N° 170-371*. 26 de septiembre de 2023a. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32413&prmTIPO=OFICIOPLEY

SGP. *Oficio N° 184-371*. 11 de octubre de 2023b. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32513&prmTIPO=OFICIOPLEY

SGP. *Oficio N° 198-371*. 25 de octubre de 2023c. pp. 2. Disponible en: https://www.camara.cl/verDoc.aspx?prmID=32601&prmTIPO=OFICIOPLEY

TEJERINA, Ofelia. *Aspectos jurídicos de la ciberseguridad*. Rama Editorial, 2020. Disponible en: https://www.digitaliapublishing.com/a/110180/aspectos-juridicos-de-la-ciberseguridad

UNITED NATIONS OFFICE ON DRUGS AND CRIME. *Estudio exhaustivo sobre el delito cibernético*. 2013. Disponible en: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

VALDEZ, Aldo. El Cibercrimen. 2009. Disponible en: https://www.researchgate.net/publication/338493033_El_Cibercrimen

PÁGINAS WEB

BEDERMAN, Uriel. La historia de John Draper, el primer “hacker malo” que engañó a los poderosos con un silbato de juguete. TN. [En línea], 03 de septiembre 2022. Disponible en: https://bit.ly/46DX7uL

COMISIÓN NACIONAL DEL MERCADO DE VALORES (CNMV). *Funciones*. [En línea] s/f, Disponible en: https://www.cnmv.es/portal/quees/Funciones/Funciones.aspx

COMISIÓN PARA EL MERCADO FINANCIERO (CMF). *Reseña histórica*. [En línea], s/f, Disponible en: https://www.cmfchile.cl/portal/principal/613/w3-article-23902.html

CSIRT. *Chile formaliza creación del CSIRT de Gobierno*. [En línea], 1 de septiembre de 2019. Disponible en: https://www.csirt.gob.cl/noticias/chile-formaliza-creacion-del-csirt-de-gobierno/

CSIRT. *Día Mundial de Internet: Hitos de la llegada de internet a Chile*. [En línea] 17 de mayo de 2022, Disponible en: https://bit.ly/3M738rM

FCA. *Insights from the 2020 Cyber Coordination Groups*. [En línea] 29 de abril de 2021, Disponible en: https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups-2020

FCA. *Our strategy 2022 to 2025*. pp. 24. [En línea] s/f, Disponible en: https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf#page=3

Financial Conduct Authority (FCA). *About the FCA*. [En línea] 19 de abril de 2016, Disponible en: https://www.fca.org.uk/about/what-we-do/the-fca

Financial Conduct Authority (FCA). *About the FCA*. [En línea] 19 de abril de 2016, Disponible en: https://www.fca.org.uk/about/what-we-do/the-fca

INE. *Población que usa Internet (en los últimos tres meses). Tipo de actividades realizadas por Internet*. [En línea] 2022, Disponible en: https://bit.ly/45DQWFR

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE). *Qué es INCIBE*. [En línea] s/f, Disponible en: https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe

NATIONAL CYBER SECURITY CENTER (NCSC). *What we do*. [En línea] s/f, Disponible en: https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

NCSC. *Annual review 2023*. [En línea] 14 de noviembre de 2023, Disponible en: https://www.ncsc.gov.uk/collection/annual-review-2023

OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS (OEDI). *Estadísticas*. [En línea] 2021, Disponible en: https://oedi.es/estadisticas/

OLMOS, Renato. *Los referentes internacionales del proyecto de ley marco de ciberseguridad*. Diario Financiero. [En línea], 31 de marzo de 2023. Disponible en: https://bit.ly/3TjOIcg

STATISTA. *Porcentaje de individuos que se conectó a Internet diariamente en el Reino Unido de 2007 a 2020*. [En línea] 2022, Disponible en: https://bit.ly/3Q7ZGhG

NORMATIVA CONSULTADA

NACIONAL:

CHILE. Decreto N.º 83, *Promulga el Convenio sobre la Ciberdelincuencia*. Diario Oficial de la República de Chile, Santiago de Chile, 28 de agosto de 2017. Disponible en: https://bcn.cl/2ij3n

CHILE. Circular N.º 2.409. 13 de diciembre de 1988. Capítulo 1-7. Disponible en: https://bcn.cl/3a6sn

CHILE. Decreto N.º 533, *Crea Comité Interministerial sobre Ciberseguridad*. Diario Oficial de la República de Chile, Santiago, Chile, 17 de Julio de 2015. Artículo 1. Disponible en: https://bcn.cl/3gbju

CHILE. Ley N.º 19.223 *que Tipifica Figuras Penales Relativas a la Informática*. Diario Oficial de la República de Chile, Santiago, Chile, 17 de junio de 1993. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=30590

CHILE. Ley N.º 19.880, *Establece Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado*. Diario Oficial de la República de Chile, Santiago de Chile, 29 de Mayo de 2003. Disponible en: https://bcn.cl/2ips6

CHILE. Ley N.º 21.000 *que crea la Comisión para el Mercado Financiero*. Diario Oficial de la República de Chile, Santiago de Chile, 27 de febrero de 2017. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1100517

CHILE. Ley N.º 21.459 *que Establece normas sobre Delitos Informáticos, deroga la ley N.º 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest*. Diario Oficial de la República de Chile, Santiago, Chile, 20 de junio de 2022. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1177743

CHILE. Ley N.º 21.521 que *Promueve la Competencia e Inclusión Financiera a través de la Innovación y Tecnología en la Prestación de Servicios Financieros* (Ley fintec). Diario Oficial de la República de Chile, Santiago, Chile, 4 de enero de 2023. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1187323

CHILE. Norma de Carácter General N.º 454. 18 de mayo de 2021, pp. 36. Disponible en: https://www.cmfchile.cl/normativa/ncg_454_2021.pdf

CHILE. Proyecto de ley marco sobre ciberseguridad e infraestructura crítica de la información. Boletín N°14.847-06. 2 de marzo de 2022. Disponible en: https://bit.ly/41x2ZEJ

CHILE. Proyecto de ley que establece normas sobre Delitos Informáticos, deroga la Ley N.º 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Boletín N.º 12.192-25, 25 de octubre de 2018. Disponible en: https://bit.ly/48awTR1

CHILE. Proyecto de ley que modifica la Ley que establece Bases de los Procedimientos Administrativos, en materia de documentos electrónicos. Boletín N.º 11882-06. 6 de julio de 2018. Disponible en: https://bit.ly/485JoxT

CHILE. Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N°11.144-07. Marzo del 2017. Artículo 30 bis, letra c. Disponible en: https://bit.ly/3fb3knt

CHILE. Proyecto de ley sobre Delito Informático. Boletín 412-07. 16 de julio de 1991. Disponible en: https://bit.ly/4abNqpM

EXTRANJERA:

CONSEJO DE EUROPA. Convenio N.º 185 *Sobre la Ciberdelincuencia*. 23 de noviembre de 2001. Disponible en: https://rm.coe.int/1680081561

ESPAÑA. DEPARTAMENTO DE SEGURIDAD NACIONAL. *Estrategia de ciberseguridad nacional*. 2013. Disponible en: https://bit.ly/488ZICS

ESPAÑA. Ley 8/2011 *de medidas para la protección de las infraestructuras críticas*, 28 de abril de 2011. Disponible en: https://www.boe.es/eli/es/l/2011/04/28/8/con

ESPAÑA. Orden PCI/487/2019 *por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional*. 26 de abril de 2019. Disponible en: https://www.boe.es/eli/es/o/2019/04/26/pci487/con

ESPAÑA. Real Decreto 1008/2017 *por el que se aprueba la Estrategia de Seguridad Nacional 2017*. 21 de diciembre de 2017. Disponible en: https://www.boe.es/eli/es/rd/2017/12/01/1008/con

ESPAÑA. Real Decreto 311/2022 *por el que se regula el Esquema Nacional de Seguridad*. 3 de mayo de 2022. Disponible en: https://www.boe.es/eli/es/rd/2022/05/03/311/con

ESPAÑA. Real Decreto-Ley 12/2018 *de seguridad de las redes y sistemas de información*, 7 de septiembre de 2018. Disponible en: https://www.boe.es/eli/es/rdl/2018/09/07/12

UNIÓN EUROPEA (UE). *Directiva 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*. Diario Oficial de la Unión Europea, 10 de julio de 2016. Disponible en: http://data.europa.eu/eli/dir/2016/1148/oj

UNIÓN EUROPEA (UE). Directiva 2022/2555 del parlamento europeo y del consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la unión, por la que se modifican el reglamento (UE) Nº 910/2014 y la directiva (UE) 2018/1972 y por la que se deroga la directiva (UE) 2016/1148 (directiva SRI 2). Diario Oficial de la Unión Europea, 27 de diciembre de 2022. Disponible en: http://data.europa.eu/eli/dir/2022/2555/oj

UNIÓN EUROPEA (UE). *Reglamento (CE) N° 460/2004 del parlamento europeo y del consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información*. Diario Oficial de la Unión Europea, 13 de Marzo de 2004. Disponible en: http://data.europa.eu/eli/reg/2004/460/oj

UNIÓN EUROPEA (UE). *Reglamento (UE) N° 526/2013 del parlamento europeo y del consejo, de 21 de mayo de 2013, relativo a la agencia de seguridad de las redes de la información de la unión europea (ENISA) y por el que se deroga el reglamento (CE) N° 460/2004*. Diario Oficial de la Unión Europea, 18 de Junio de 2013. Disponible en: http://data.europa.eu/eli/reg/2013/526

UNIÓN EUROPEA (UE). *Reglamento 2019/881 del parlamento europeo y del consejo, de 17 de abril de 2019, Relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la Ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) N° 526/2013 («Reglamento sobre la Ciberseguridad»)*. Diario Oficial de la Unión Europea, 7 de junio de 2019. Disponible en: http://data.europa.eu/eli/reg/2019/881/oj

UNION EUROPEA (UE). *Reglamento 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de*

Coordinación. Diario Oficial de la Unión Europea, 8 de Junio de 2021. Disponible en: http://data.europa.eu/eli/reg/2021/887/oj

UNION EUROPEA. *COM 2000/890 final. Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. 2001. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

UNION EUROPEA. *COM 2002/173 final. Propuesta de Decisión-marco del Consejo relativa a los ataques de los que son objeto los sistemas de información*. 2002. Disponible en: https://www.europarl.europa.eu/meetdocs/committees/libe/20020522/173000es.pdf