CIBERSEGURIDAD EN EL DERECHO CHILENO: ESTADO, DESAFÍOS Y PROYECCIONES

CYBERSECURITY IN CHILEAN LAW: STATUS, CHALLENGES AND PROJECTIONS

DOI: 10.19135/revista.consinter.00020.13
Recibido/Received 31/12/2024 – Aprobado/Approved 27/03/2025

Bárbara Cortés Cabrera[1] *– https://orcid.org/0009-0009-2687-7293*
Christian Scheechler Corona[2] *– https://orcid.org/0000-0002-2251-0250*

Resumen

El artículo analiza el nuevo contexto normativo de la ciberseguridad en Chile, con el objetivo de reflexionar sobre sus alcances, limitaciones y desafíos, con especial énfasis en las amenazas generadas por los delitos informáticos y la ciberdelincuencia. Se plantea como hipótesis que, pese a los importantes avances normativos alcanzados, aún persisten desafíos para abordar los retos en una sociedad altamente digitalizada, que permitan la construcción de un ciberespacio seguro y regulado.

Mediante un enfoque cualitativo, se efectúa una aproximación descriptiva de la sociedad digital y un análisis crítico del actual marco normativo nacional, con ciertas aproximaciones al marco internacional, así como de la doctrina especializada. A través del método dogmático, se presenta un cuadro una reflexión en torno a un mínimo marco normativo necesario para un ciberespacio seguro, comenzando por la incorporación de figuras penales contempladas en el Convenio de Budapest y de estándares en materia de ciberseguridad, protección de datos y protección de infraestructura crítica. Finalmente, se concluye que persisten retos como la dispersión normativa, la limitada cooperación internacional en la persecución delictual transfronteriza y la ausencia de figuras penales que incluyan adecuadamente ciertos fenómenos de ciberdelincuencia.

Palabras claves: Ciberseguridad; Derecho Penal; Delitos informáticos; Ciberdelitos.

Abstract

The article analyzes the new regulatory context of cybersecurity in Chile, with the aim of reflecting on its scope, limitations and challenges, with special emphasis on the threats generated by computer crimes and cybercrime. It is hypothesized that, despite the significant regulatory advances achieved, challenges remain in addressing the challenges in a highly digitized society that would allow for the construction of a safe and regulated cyberspace.

Through a qualitative approach, a descriptive approximation of the digital society is made and a critical analysis of the current national regulatory framework, with certain approximations to the international framework, as well as of the specialized doctrine. Based on the dogmatic method, a reflection is presented on the minimum regulatory

[1] Doctoranda en Derecho por la Universidad Complutense de Madrid, España, código postal 28008, bacortes@ucm.es, ORCID https://orcid.org/0009-0009-2687-7293

[2] Doctor en Derecho por la Universidad de Deusto, Profesor de Derecho Penal en la Facultad de Derecho de la Universidad Católica de la Santísima Concepción, Concepción, Chile, código postal 4090541, cscheechler@ucsc.cl, ORCID https://orcid.org/0000-0002-2251-0250.

framework necessary for a secure cyberspace, starting with the incorporation of criminal offenses contemplated in the Budapest Convention and standards on cybersecurity, data protection and critical infrastructure protection. Finally, it is concluded that challenges persist, such as regulatory dispersion, limited international cooperation in cross-border criminal prosecution and the absence of criminal offenses that adequately include certain cybercrime phenomena.

Keywords: Cybersecurity; Criminal Law; Digital Law; Computer crimes; Cybercrime.

Sumario: 1. Introducción. 2. Ciberespacio como dimensión jurídicamente relevante. 3. Vulnerabilidades del ciberespacio, amenazas y ciberseguridad. 4. Delitos informáticos, ciberdelitos y ciberseguridad en el derecho penal chileno. 4.1. Breves antecedentes sobre los delitos informáticos y los ciberdelitos. 4.2. La legislación sobre delitos informáticos en Chile, en particular la Ley 21.459. 4.3. Los delitos informáticos actualmente vigentes en la legislación chilena. 5. Actualidad y contexto normativo de ciberseguridad en Chile. 6. Conclusiones. 7. Referências.

1 INTRODUCCIÓN

A esta altura del desarrollo tecnológico, podemos sostener cierto acuerdo en que el tiempo de los "desafíos de la computación", o incluso de la propia informática, ya son cosa del pasado (reciente, pero pasado). La creciente sofisticación de los delitos informáticos y la expansión del cibercrimen han exigido respuestas jurídicas más eficaces y actualizadas por parte de los Estados.

En ese escenario, los primigenios delitos computacionales dieron paso a nuevos fenómenos delictivos, que han sido captados, en mayor o menor medida, por tipos penales especiales en diversas legislaciones. Pero la respuesta a estos fenómenos está lejos de ser solo de Derecho Penal, o al menos de Derecho Penal sustantivo. Las amenazas a personas naturales, empresas, grupos intermedios en general y al Estado, han configurado un entorno que provoca una respuesta estatal multidimensional. Así, a las herramientas del "viejo y querido Derecho Penal liberal", y del Derecho Procesal tradicional, se han ido agregando algunas de carácter transnacional (con la Unión Europea, en adelante "UE", como pionera) y otras técnico-normativas. Aquí es donde aparece la idea de ciberseguridad, en tanto concepto poliédrico e institución compleja.

Chile, como miembro de la Organización para la Cooperación y el Desarrollo Económico (en adelante, "OCDE") y actor relevante en el ámbito latinoamericano, ha adoptado un enfoque modernizador en materia de ciberseguridad, mediante la promulgación de diversas leyes en la materia. Pese a la reciente modernización, Chile aún enfrenta desafíos que dificultan una respuesta integral frente a las amenazas digitales, lo que exige un análisis crítico y propositivo sobre la actual estructura legislativa y sus posibles mejoras, para la consolidación de un ecosistema digital seguro y resiliente.

El presente estudio tiene como objetivo analizar el nuevo escenario normativo de la ciberseguridad en Chile, reflexionando entorno a sus alcances y desafíos, particularmente en lo que respecta a los delitos informáticos. En este contexto, la hipótesis de investigación que se plantea sostiene que, si bien las reformas legales han representado un avance significativo en el tejido normativo del ciberespacio, la ausencia de una estrategia integral de ciberseguridad deja en

evidencia un conjunto de falencias que obstaculizan la construcción de un ciberespacio seguro.

Para abordar estos cuestionamientos, bajo un procedimiento metodológico, el estudio que se presenta adopta un enfoque cualitativo, basado en el análisis crítico de normas nacionales e internacionales y la doctrina especializada, utilizando los métodos dogmáticos tradicionales (exegético-sistemático). Desde un diseño descriptivo y analítico, se examina la evolución del marco normativo chileno en ciberseguridad y su adecuación a la luz de estándares internacionales.

En el presente trabajo, abordaremos de forma breve el estado de la cuestión en materia de ciberespacio, y como este se ha consolidado como una dimensión propicia para la comisión de delitos, donde el Estado, regulador por excelencia, ha debido construir herramientas jurídicas ad-hoc a su naturaleza. Luego, repasaremos de forma descriptiva, algunas de estas ciberamenazas, para decantar en la legislación chilena sobre ciberdelincuencia. Finalmente, convergeremos en la situación actual en materia de ciberseguridad en Chile, con una mirada puesta en los desafíos venideros frente a los cambios actuales.

Como conclusión, frente a la fragmentación legislativa, a la insuficiente cooperación internacional y ante la ausencia de figuras penales específicas, se plantea la necesidad de consolidar un marco normativo integral y coordinado, que garantice una mejor articulación institucional frente a las amenazas digitales, que refuerce la cooperación internacional y actualice la tipificación de los delitos informáticos para enfrentar de manera efectiva los riesgos de la sociedad digital.

2 EL CIBERESPACIO Y SU DESARROLLO COMO DIMENSIÓN JURÍDICAMENTE RELEVANTE

En la historia de la humanidad no había ocurrido un evento tan transformador de la sociedad como la aparición de Internet. Si bien, la Revolución Industrial significó un catalizador de la evolución global, no es posible compararlo con lo que Internet ha gatillado, una gran transformación global a nivel tecnológico, cultural, económica, política y social.

El desarrollo de Internet y otras redes informáticas y telemáticas, en convergencia con el surgimiento de otras tecnologías, propició la creación de un espacio virtual de interacción, de intercambio de información e internacionalización de la interconexión. Este nuevo escenario es un presupuesto básico de la globalización[3] y de la sociedad de la información, caracterizado por la transmisión transfronteriza de la información[4] y de suministro de servicios[5], como resultado de

---

[3] IBÁÑEZ MUÑOZ, Josep, "Globalización e Internet: poder y gobernanza en la sociedad de la información", *Revista Relaciones Internacionales*, n.4, 2006, pp. 1-33. De acuerdo a Ibáñez, la globalización es *la progresiva transformación de un conjunto de procesos sociales interrelacionado (económicos, políticos, culturas, medioambientales) cuya intensidad aumenta y se manifiesta en una escala geográfica que tiende a ser mundial.*

[4] CASTELLS OLIVÁN, Manuel, "Globalización, Estado y sociedad civil: El nuevo contexto histórico de los derechos humanos", *Revista Isegoría*, n. 22, 2000, p.5.

[5] MUÑOZ MACHADO, Santiago, *La regulación de la Red. Poder y Derecho en Internet*, Madrid, Editorial Taurus, 2000, p. 42. De acuerdo a Muñoz Machado, *el desarrollo de la tecnología ha contribuido a la multiplicación de los efectos de la globalización*.

un proceso global, multidisciplinario y dinámico, motivado por un sistema tecnológico de información y de telecomunicaciones.

Sin embargo, así como se ha potenciado el desarrollo en todas las dimensiones, también se han abierto ventanas para nuevas amenazas para la ciudadanía, organizaciones y Estados, siendo esto último un fenómeno especialmente sensible.

La necesidad de comprender el ciberespacio ha enfrentado a la doctrina y a las instituciones gubernamentales en la discusión sobre su naturaleza jurídica. A modo de contexto, recordemos que los orígenes de Internet están marcados por una corriente autócrata de libre regulación[6], aunque quedó atrás para dar paso a un marco regulatorio que además protegiera los derechos fundamentales.

Desde una aproximación formal al concepto, la Real Academia Española define al Ciberespacio como el "ámbito virtual creado por medios informáticos"[7]. De ella es posible desprender que se trata de un escenario inmaterial e intangible, creado artificialmente por medios informáticos, es decir, por el ser humano. Sin embargo, llama la atención que no indica cómo se puede habitar dicho espacio, ni las actividades que se pueden desarrollar en él, ni su proyección global ni su vinculación con el ámbito real[8].

Naturalmente, el ciberespacio ha evolucionado y se plantea como:

> *"Un nuevo orden fundado en un lenguaje programado propio basado en dígitos, conformado por una comunidad cibernauta con unos poderes económicos y de impacto social desproporcionados (operadores de buscadores, plataformas digitales centralizadas y redes sociales), y en un territorio diáfano e ilimitado (Internet y sus "dominios"), esto es, una extensa red con estratos superpuestos a modo de un iceberg (surface web – Deep web – Darknet- darkweb), de difícil acceso los más profundos para unos usuarios con unas capacidades digitales medias. Por último, este nuevo mundo se racionaliza a través de inteligencia artificial, algoritmos nutridos de grandes masas de datos, los mega – datos (Big data), la ´materia prima digital´ obtenida de la amalgama de relaciones entre sujetos y organizaciones, públicas y privadas que se entablan en este cosmos artificial"*[9].

---

[6] Para los ciberlibertarios, Internet era un espacio emergente e independiente al espacio físico, ajeno a los marcos normativos tradicionales y donde no se podría aplicar la legislación. Así lo plasmó John Perry Barlow en su Declaración de Independencia del Ciberespacio de 1966. Esta discusión se trasladó al campo jurídico cuestionando la aplicación de la tradicional Teoría del Estado. En "Law and Borders – the Rise of Law in Cyberspace", David Johnson y David Post sostenían que dado que las fronteras trazadas en el espacio físico delimitan el "espacio jurídico" – donde se aplican las normas jurídicas- y el ciberespacio carece de fronteras, no es posible someterlo a un régimen jurídico determinado, sino que debía contar con un marco regulatorio adecuado a sus características.

[7] REAL ACADEMIA DE LA LENGUA ESPAÑOLA, *Ciberespacio. Diccionario de la Lengua Española,* Edición del Tricentenario, Disponible en: https://dle.rae.es/ciberespacio?m=form, Acceso en: 30 dic. 2024.

[8] Actualmente, la utilización del prefijo "ciber" goza de amplia aplicación y se asocia a las relaciones que trascienden el contacto físico de la territorialidad, en un espacio emergente de interacción no concreto que tiene que ver con ordenadores y redes, aplicándose a diferentes a eventos en el ciberespacio, tales como "ciberentorno", "ciberterrorismo", "ciberataque", "cibernauta", "ciberseguridad", "ciberdefensa", "ciberdelitos", entre otros.

[9] CANALS AMETLER, Dolors, *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales*, primera edición, Madrid, Editorial El Consultor De Los Ayuntamientos, 2021, p.66.

A partir de la propuesta contingente de Canals, se desprende que el ciberespacio se ha forjado como una nueva estructura socioeconómica con una particularidad esencial que contribuye a la sociedad digital. Nos referimos a que, en el ciberespacio, a partir de las interacciones de los usuarios y organizaciones, se genera información que es posteriormente procesada a través de inteligencia artificial (IA) y algoritmos que utilizan grandes volúmenes de datos (Big Data). En la actualidad, los datos son el principal insumo de organizaciones públicas y privadas y, asimismo, es la materia prima que por antonomasia emana de la navegación en Internet.

La relación entre el espacio virtual y material también se observa en la estructura del ciberespacio, que se compone de tres capas: una capa física, que corresponde al hardware que permite materialmente la transmisión de información; una capa "lógica" que permite la conexión gracias a los protocolos de comunicación; y una tercera capa, de los "servicios y contenidos", integradas por las múltiples fuentes de información y conocimiento, así como los servicios que se prestan en línea[10]. De estas, la única capa visible para la generalidad de los usuarios es la *Surface web* (la capa más visible) a la que se puede acceder desde los motores de búsqueda comunes, el resto es parte de la gran nebulosa donde ocurren las ciberamenazas. Sin embargo, estas capas no son compartimientos estancos, pues lo que ocurre en el espacio virtual repercute en el espacio material.

Así las cosas, el ciberespacio se caracteriza por su espacio transfronterizo, por su ausencia de soberanía, difusa jurisdicción, fácil acceso y posibilidad de actuar en clandestinidad, difícil atribución de acciones delictuales y débil regulación[11]. Este espacio sin fronteras comparte la esencia de aquellos que han sido denominados por la doctrina como "espacio común global"; sin embargo, por su naturaleza inmaterial, repercute en el derecho procesal por la compleja delimitación del ámbito de la aplicación de la ley y de la jurisdicción del Estado.

3 VULNERABILIDADES DEL CIBERESPACIO, AMENAZAS Y CIBERSEGURIDAD

El desarrollo de Internet y de las TIC´s han sido esenciales para el progreso de la sociedad, pero también una oportunidad para inescrupulosos navegadores del ciberespacio. La ausencia de un espacio físico lo ha convertido en una dimensión de encuentro virtual y de intercambio de información, en que fácilmente es posible ocultar la identidad, facilitando la comisión de delitos a un bajo costo económico.

Como indicábamos, la ausencia de fronteras físicas en el ciberespacio y la débil jurisdicción dificultan la persecución de ciberataques. Asimismo, en consideración a que la regulación varía de Estado en Estado, también se presentan dificultades en la estandarización regulatoria, afectando a la legalidad de las actividades en el ciberespacio, es decir, lo que en un Estado podría ser ilícito en otro Estado no lo es.

---

10 BARRIO ANDRÉS, Moisés, *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*, Valencia, Editorial Tirant Lo Blanch, 2018, p. 25.

11 PÉREZ BES, Francisco, *Memento experto ciberseguridad*, Madrid, Editorial Francis Lefebvre, 2021, p. 22.

En el ciberespacio, como respuesta a las ciberamenazas ha surgido la ciberseguridad. Esta última se centra en proteger los sistemas y redes informáticas frente a accesos no autorizados, robos, daños o cualquier actividad maliciosa; las ciberamenazas son aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Dentro de sus particularidades, destacan el bajo costo que representa su utilización, la facilidad de ejecución con impactos transfronterizos y la baja probabilidad de identificación del atacante, entre otros[12].

De las ciberamenazas pueden emanar diferentes acciones que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas información interconectados, tales como el ciberespionaje, amenazas híbridas, cibercrimen, ciberterrorismo, "hacktivismo" y campañas de desinformación. Todas ellas pueden considerarse dentro del concepto de cibercriminalidad, que abordaremos *infra*, y que se puede manifestar en diversas modalidades[13].

Los ciberdelitos y/o delitos informáticos utilizan las tecnologías digitales para cometer actos ilícitos que pueden afectar a individuos o entidades públicas o privadas, y en general se subsumen en diferentes tipos penales. Dentro de estos últimos, se reconocen las violaciones de la privacidad, pornografía infantil, incitación al odio y a la violencia en línea, delitos financieros, robos de identidad, acceso no autorizado a la información contenida en sistemas de información, como su modificación y sustracción, entre muchos otros.

Por otro lado, el ciberterrorismo comprende acciones de organizaciones terroristas o afines, con la finalidad de realizar actividades de propaganda, comunicaciones internas, formación, adoctrinamiento, financiación, reclutamiento y obtención de información, y causar terror en la población a través de ataques a la infraestructura crítica.

Por último, y sin ánimo de taxatividad, el "hacktivismo" comprende acciones que, bajo la apariencia de una causa social, política o ideológica, persigue ocasionar un impacto negativo en la imagen de terceros a través del ingreso no autorizado y control de los sistemas informáticos, interrupción de servicios, difusión de información personal, etc.

En las últimas décadas, el ciberespacio ha sido el lugar donde más se han presentado amenazas a los gobiernos, empresas, organizaciones no gubernamentales, y también a particulares. La delincuencia – y, por cierto, la ciberdelincuencia- está en permanente evolución, logrando ofensivas cada vez más sofisticadas, económicas y perjudiciales.

Para hacer frente a esta compleja realidad, surge la ciberseguridad como una respuesta para proveer seguridad, configurándose como un concepto poliédrico, multidimensional y en permanente evolución.

De acuerdo a la Unión Internacional de Telecomunicaciones (UIT), siguiendo la Recomendación UIT-T X.1205, la ciberseguridad es *"*un conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno*"*. Suscribimos a esta amplia

---

12 PÉREZ BES, Francisco, *Memento experto ciberseguridad*, Madrid, Editorial Francis Lefebvre, 2021, p. 10.

13 PÉREZ BES, Francisco, *Memento experto ciberseguridad*, Madrid, Editorial Francis Lefebvre, 2021, p. 133.

comprensión de ciberseguridad, pues aborda desde la seguridad de la infraestructura nacional y de las redes, hasta la seguridad o integridad de los usuarios[14].

En el mismo sentido, esta concepción de la ciberseguridad también fue recogida en el Reglamento sobre Ciberseguridad de la Unión Europea[15], que en el art. 2.1º la define como *"*todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas*"*. Así, los países miembros de la UE suscriben a la posición que la ciberseguridad es una actividad que se integra tanto en la seguridad pública (por lo tanto, también es un pilar de la Seguridad Nacional), como en telecomunicaciones e infraestructura crítica.

El abordaje de la ciberseguridad desde diversos ámbitos no es baladí pues, aunque su surgimiento se asocia a la protección de las infraestructuras, redes y sistemas de información (ataques a sistemas, datos, propiedad intelectual, menores y seguridad), la actividad en el ciberespacio también puede afectar a los derechos fundamentales.

Como se puede inferir, la ciberseguridad no es un fin en sí misma, es una condición que permite el ejercicio de otros derechos fundamentales, y cuya competencia recae en el Estado Así , "la dignidad de la persona, la libertad ideológica o de expresión, la intimidad, el honor, los servicios sociales o, incluso, la propiedad privada, entre otros derechos, pueden verse, comprometidos cuando los sistemas de información que sustentan su ejercicio práctico dejan de funcionar o lo hacen de manera irregular, como consecuencia de las acciones deliberadas que los agentes de las amenazas desarrollan*"*[16].

Naturalmente, asumir el rol que tiene el Estado en materia de ciberseguridad nos impulsa a repensar los elementos que tradicionalmente componen el Estado, pero que en la nueva realidad digital se ven afectados, tales como el territorio, soberanía y ciudadanía. Como se ha señalado anteriormente, el ciberespacio tiene sus particularidades, no tiene fronteras y pone en encrucijada el principio de territorialidad; por otra parte, en un espacio artificial transfronterizo donde no es posible ejercer la soberanía, por lo que se ha planteado avanzar hacia la construcción de una soberanía digital [17/18], y finalmente, en el ciberespacio no existen ciudadanos

---

14 ASOCIACIÓN POR LOS DERECHOS CIVILES, *Descubriendo la agenda de ciberseguridad de Latinoamérica: el caso de Argentina, ¿Qué entendemos por ciberseguridad?*, primera entrega, Ottawa, Cyber Stewards Network, 2015, Disponible en: https://adc.org.ar/wp-content/uploads/2019/06/007-A-descubriendo-la-agenda-de-ciberseguridad-de-america-latina-el-caso-argentina-1ra-entrega-10-2015.pdf, Acceso en: 30 dic. 2024.

15 PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, "Artículo 2" *en* Parlamento Europeo y del Consejo, org., *Reglamento (UE) 2019/881 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) Nº 526/2013 (Reglamento sobre la Ciberseguridad)*, Estrasburgo, Unión Europea, 2019, Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019R0881, Acceso en: 30 dic. 2024.

16 DOMÍNGUEZ ÁLVAREZ, José Luis, "Derecho a la seguridad digital: génesis, evolución y perspectivas de futuro" *en* RODRÍGUEZ AYUSO, Juan, org., *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Navarra, Editorial Thomson Reuters Aranzadi, 2022, p.103

17 FABA DE LA ENCARNACIÓN, Elena, SIMON CANAL, Tomás, "Soberanía digital: ¿Un problema normativo o un problema geopolítico?", *Revista de Economía Industrial: Soberanía Tecnológica e Industrial*, n.427, 2023, p. 45. De acuerdo a Elena Faba de la Encarnación y Tomás Simón, la soberanía digital *es la capacidad que tiene un Estado para proteger e incidir en el uso y gestión de los datos e información que se generan en su territorio fruto del uso de las tecnologías por parte de sus ciudadanos.*

como tales, pues dicha noción está ligada a la nacionalidad, cuestión que también se encuentra en encrucijada en el ciberespacio por su naturaleza globalizada.

4 DELITOS INFORMÁTICOS, CIBERDELITOS Y CIBERSEGURIDAD EN EL DERECHO PENAL CHILENO

4.1 Breves Antecedentes Sobre los Delitos Informáticos y los Ciberdelitos

La situación en Chile no dista demasiado de lo descrito hasta el momento, con avances y retrocesos. La reciente ley publicada en Chile el año 2022 mantiene en lo esencial la nomenclatura usada ya hace más de tres décadas, en 1993, con la hoy derogada Ley N° 19.223, que tipificaba figuras "relativas a la informática". No deja de ser llamativo que, bien entrado el Siglo XXI, el legislador se mantiene anclado a una nomenclatura que parece superada. Esa es básicamente la razón por la que Romeo Casabona habla de una siguiente generación de delitos posterior a los informáticos, caracterizados por la presencia de las redes telemáticas, como son los ciberdelitos. El concepto del autor es eminentemente cualitativo, como se verá con posterioridad[19].

Sin embargo, él mismo advierte que el término cibercrimen o ciberdelito tampoco es completa ni totalmente preciso desde una perspectiva penal, por lo que se obstaculiza la finalidad de cumplir con una función integradora a las expresiones criminógenas asociadas a las TICs, al menos desde un punto de vista dogmático. Lo que sí permitiría con mayor facilidad es un enfoque criminológico de la situación, al ser lo suficientemente flexible como para responder a las características fenomenológicas del conjunto de conductas usualmente consideradas[20].

A propósito de esto último, cabe hacer presente que la distinción entre delitos informáticos y ciberdelitos parece alcanzar también a los países angloparlantes. Ya en 1983, un grupo de expertos de la OCDE utilizó el término *computer-related crime* o delitos relacionados con los ordenadores, entendiendo por tales cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos[21]. Más común es el uso de la expresión *computer crime*, concepto que traducido al español significa por igual delitos

---

[18] De acuerdo a Tamara Robles, la soberanía digital es la "capacidad de ejercer control sobre el propio espacio digital" . En ÁLVAREZ ROBLES, Tamara, *El Derecho de acceso a Internet. Especial referencia al Constitucionalismo español*, Valencia, Editorial Tirant Lo Blanch, 2024, p. 52.

[19] ROMEO CASABONA, Carlos, "De los delitos informáticos al cibrecrimen. Una aproximación conceptual y político-criminal" *en* ROMEO CASABONA, Carlos, org., *El Cibercrimen. Nuevos retos jurídicos-penales, nuevas respuestas político-criminales*, Granada, Editorial Granada Comares, 2006, p.9.

[20] ROMEO CASABONA, Carlos, "De los delitos informáticos al cibrecrimen. Una aproximación conceptual y político-criminal" *en* ROMEO CASABONA, Carlos, org., *El Cibercrimen. Nuevos retos jurídicos-penales, nuevas respuestas político-criminales*, Granada, Editorial Granada Comares, 2006, p.9.

[21] Concepto valorado por Sieber debido a su amplitud, lo que permite ser utilizado tanto desde una perspectiva dogmática penal como criminológica o policial, por ejemplo, SIEBER, Ulrich, "Documentación para una aproximación al delito informático" en MIR PUIG, Santiago, org., *Delincuencia informática*, Barcelona, Editorial Promociones y Publicaciones Universitarias, 1992, p. 66.

computacionales o delitos informáticos[22], cuestión que sin duda ha influido en las dificultades de la doctrina de habla hispana para encontrar los términos adecuados.

Sieber prefiere la utilización del término delitos informáticos[23], y aunque no lo define, sí ejemplifica algunas de las formas de realización de estas figuras y que eran de común ocurrencia, principalmente en la década del ochenta. Entre estas se cuentan manipulaciones de ordenador (*input, software*, consola, *output* y abusos especiales en tiempo compartido o teleproceso), espionaje informático y hurto de *software*, sabotaje informático, hurto de tiempo y delitos económicos en general[24].

El concepto de delitos informáticos es impreciso, pues como bien recuerda Rovira Del Canto, nace de la traducción semiliteral del anglicismo *computer crimes*, que alude al medio comisivo –computador u ordenador- y no a la ciencia que procura su funcionamiento –la informática, o mal llamada coloquialmente como computación-[25].

Crítico de este concepto de delito informático, Romeo Casabona apunta a que no puede hablarse del tema en singular[26], toda vez que se trataría de una pluralidad de conductas cuyo único punto común es su vinculación de alguna manera con los ordenadores[27]. La visión del autor en este sentido es correcta, pues la mayor parte de los esfuerzos que buscan unificar conceptos en este sentido tienden a utilizar criterios demasiado amplios, que desfiguran los contornos del objeto que se pretende definir. Romeo Casabona opta por expresiones como "delincuencia informática" o "delincuencia vinculada al ordenador o a las tecnologías de la información"[28]. El mismo autor entrega los rasgos generales sobre los que debería trabajarse: "A la vista de estas definiciones podemos concluir que la delincuencia informática o los delitos relacionados con la misma indican un aspecto de la criminalidad que, caracterizado por una *nueva dimensión* que explica su *especificidad*, ambas notas las aporta el ordenador junto con sus *funciones propias* más importantes: el

---

22 Incluso, según el Diccionario de Oxford, podría utilizarse hasta como idea afín de Internet, en algunas oraciones. OXFORD DICTIONARIES, *Oxford Languages,* Disponible en: <http://www.oxforddictionaries.com/es/traducir/ingles-espanol/computer>, Acceso en: 29 dic. 2024.

23 Otros autores se refieren al concepto en singular, es decir, delito informático. Véase, entre otros, BLAS ZULUETA, Luis, "Delitos informáticos", *Revista General de Derecho*, n. 495, 1985, pp. 310 – 311; BOLAÑOS RAMÍREZ, M.R., "El delito informático como nueva figura jurídica", *en* AAVV, org., *Actas del Primer Congreso Iberoamericano de Informática Jurídica*, Madrid, Editorial CREI, 1985, pp. 301 – 302; CAMACHO LOSA, Luis, *El delito informático*, Madrid, Editorial Gráficas Cóndor, 1987, pp. 5 y 6, entre otros.

24 SIEBER, Ulrich, "Criminalidad informática: peligro y prevención" *en* MIR PUIG, Santiago, org., *Delincuencia informática*, Barcelona, Editorial Promociones y Publicaciones Universitarias, 1992, pp. 15 – 16.

25 ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Granada, Editorial Comares, 2002, p. 29.

26 Puede apreciarse de este modo en ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Granada, Editorial Comares, 2002, p. 159 y ss.; CRUZ DE PABLO, José, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, Madrid, Editorial Grupo Difusión, 2006, p. 20; AGUILAR CÁRCELES, Marta, "Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido", *Revista Cuadernos de Política Criminal*, n. 110, 2013, p. 233; entre otros.

27 ROMEO CASABONA, Carlos, *Poder informático y seguridad jurídica,* Madrid, Editorial Fundesco, 1987, p. 41. En igual sentido, MATA Y MARTÍN, Ricardo, *Delincuencia informática y derecho penal*, Madrid, Editorial Edisofer, 2001, pp. 21-23.

28 ROMEO CASABONA, Carlos, *Poder informático y seguridad jurídica,* Madrid, Editorial Fundesco, 1987, p. 41.

procesamiento y transmisión automatizados de datos y la confección y/o utilización de programas para tales fines"[29].

No obstante, ya en la década del ochenta, el propio Romeo Casabona y otros autores comprendían que la terminología ocupada hasta ese momento en habla hispana no era precisa en términos jurídicos para definir el fenómeno estudiado. La gama de conductas relacionadas con las nuevas tecnologías tentaba a la doctrina a insistir en conceptos amplios, que permitieran la inclusión de estos comportamientos. Los ataques de los *hackers* y *crackers* suponían la existencia de hechos no solamente patrimoniales, sino que afectaban otros intereses no contemplados hasta ese momento, a los que se agregaban manipulaciones en cajeros, abusos en las telecomunicaciones y ataques a la privacidad. Sieber era uno de los partidarios de este concepto amplio, por su capacidad inclusiva frente al nuevo escenario[30].

Gutiérrez Francés, en principio, se inclina por la fórmula defendida por Sieber, es decir, un concepto amplio, ya que una herramienta conceptual menos rígida abarcaría las características criminológicas del fenómeno, y permitiría incluir no solo las conductas tipificadas, sino aquellas merecedoras de tal. Así, la autora acepta denominaciones como criminalidad informática, delincuencia vinculada a los sistemas de procesamiento de datos u otras similares[31]. Sin embargo, debemos recalcar que esto es solo un punto de vista inicial, toda vez que la misma Gutiérrez Francés afirma que debe agregarse a ese concepto amplio criterios correctivos que permitan delimitar su contenido, buscando especificidad en la relación de los medios informáticos con los delitos en cuestión[32/33].

Cruz De Pablo define delito informático como, "[…] aquellas conductas típicas, antijurídicas, culpables, y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores, computadoras o cualquier otro mecanismo electrónico o informático, bien como medio, bien como

---

[29] *Ibíd*, p. 43 (cursivas del autor). El mismo autor, años después, describiría a los delitos informáticos como "conductas que atentan de forma grave a determinados bienes del individuo –pero también de personas jurídicas- que presentan una configuración específica y exclusiva de la actividad informática y telemática, y han sido sometidos a una tipología técnico-criminológica". LUZÓN PEÑA, Diego, *Enciclopedia penal básica,* Granada, Editorial Comares, 2002, p. 518.

[30] SIEBER, Ulrich, *The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy*, Michigan, Editorial Wiley, 1986, p. 19, Manual internacional sobre delitos informáticos: delitos económicos relacionados con la informática y violaciones de privacidad. Este carácter amplio puede apreciarse en la definición entregada por la Reunión de Expertos en el Ciberdelito, de la Organización de Estados Americanos, del año 2003, que entiende por delito informático (se insiste en el singular) como "[…] toda conducta, atentatoria de bienes jurídicos relevantes, que suponga el uso de medios informáticos en alguna de sus fases de ejecución". ORGANIZACIÓN DE ESTADOS AMERICANOS, *Reunión de Expertos en el Ciberdelito*, 2003, Disponible en: https://www.oas.org/es/, Acceso en: 30 dic. 2024.

[31] GUTIÉRREZ FRANCES, María Luz, *Fraude informático y estafa (aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos),* Madrid, Editorial Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, 1991, p. 53.

[32] GUTIÉRREZ FRANCES, María Luz, *Fraude informático y estafa (aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos),* Madrid, Editorial Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, 1991, p. 53.

[33] En similar sentido, BEQUAI, August, *Computer crime,* Lexington, Editorial Health Lexington Books, 1978, pp. 3 y ss, Crimen informático. Ver también, TORTRAS Y BOSCH, Carlos, "El delito informático", *Revista Informática y Derecho,* n. 17, 1989, p. 45.

fin, o mediante el uso indebido de los mismos"[34]. Esta definición refleja, a través de sus medios comisivos, la ausencia aún de la idea de redes informáticas o telemáticas, poniendo el acento más bien en los *hardwares* utilizados para la actividad delictiva, como ordenadores u otros mecanismos "electrónicos", o sobre los que recae alguna conducta.

Surge en la evolución de los delitos informáticos un concepto que causa cierta confusión en términos de nomenclatura, al ser utilizado muchas veces como sinónimos. Se trata de ciberdelitos o cibercrimen. Romeo Casabona lo considera *a priori* como un conjunto de conductas de una generación posterior a los delitos informáticos, cuyas características se verán *infra*. En primera instancia se comparte esta apreciación en lo general, pero con algunas variantes específicas en cuanto a extensión[35].

Los primeros, de acuerdo con lo descrito por el mismo autor y otros ya citados, se caracterizarían por el uso de la informática como medio comisivo y/o como objeto de la conducta. Sin embargo, la nota característica de los ciberdelitos sería la incorporación de redes de comunicación y sistemas telemáticos para la comisión de los ilícitos. Algo similar ocurre en la literatura anglosajona, donde es posible hacer una distinción entre *cyber crime* (separados) y *cybercrime* (escrito sin separación).

El primer concepto reflejaría los modos convencionales de actuación mediante el empleo de nuevas tecnologías, mientras que, escrito como un solo vocablo, haría alusión a nuevas formas de criminalidad mediante el uso de tales tecnologías, como el *cibergrooming* o el ciberterrorismo, por ejemplo[36]. Es este grupo de figuras el que da también un nuevo alcance a los problemas de seguridad informática, y por el que hablamos de ciberseguridad.

4.2 La Legislación sobre Delitos Informáticos en Chile, en Particular la Ley 21.459

Como habíamos anticipado, la legislación chilena vigente en materia de delitos asociados a la informática y la telemática parece haber dado un paso modernizador frente a la ya vetusta Ley 19.223 (que, digámoslo, fue innovadora a nivel continental en su momento). Sin embargo, una muy rápida revisión da cuenta de una nomenclatura superada y de importantes ausencias en su articulado. Como bien identifica Mayer, no existen referencias a Internet ni a las redes informáticas, sino que se mantiene dentro de los conceptos de datos o sistemas informáticos[37], igual como lo hacía su predecesora.

---

34 CRUZ DE PABLO, José, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, Madrid, Editorial Grupo Difusión, 2006, p. 20.

35 ROMEO CASABONA, Carlos, "De los delitos informáticos al cibrecrimen. Una aproximación conceptual y político-criminal" *en* ROMEO CASABONA, Carlos, org., *El Cibercrimen. Nuevos retos jurídicos-penales, nuevas respuestas político-criminales*, Granada, Editorial Granada Comares, 2006, p.6.

36 SMITH, Russell, GRABOSKY, Peter, URBAS, Gregor, *Cyber criminals on trial*, Cambridge, Editorial University Press, 2004, pp. 5-6. Ciberdelincuentes en juicio.

37 MAYER LUX, Laura, "El cibercrimen en tiempos de la nueva ley de delitos informáticos" *en* SCHEECH-LER CORONA, Christian, org*., Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones, p. 37.

Un aspecto curioso de esta observación es que el antecedente directo y cercano en el tiempo más importante para esta ley es el Convenio sobre la Ciberdelincuencia del Consejo de Europa, del año 2004, popularmente conocido como el Convenio de Budapest, por la ciudad en que se firma. El instrumento fue ratificado por Chile y promulgado vía Decreto 83 del Ministerio de Relaciones Exteriores, con fecha 27 de abril del 2017, entrando en vigor el día 28 de agosto de ese año. El Convenio, como su nombre lo dice, tiene por objeto diversas conductas y fenómenos propios de la ciberdelincuencia, incluyendo lo que tradicionalmente hemos entendido por delitos informáticos, pero superándolos con creces.

Así, por ejemplo, los dos primeros títulos del Convenio, artículos 1 a 8, están centrados en los datos y los sistemas informáticos, con delitos como el sabotaje o el acceso ilícito. Luego, el Título 3 tratan sobre los delitos relacionados con los contenidos, y allí encontramos los delitos de pornografía infantil (el Convenio usa dicha nomenclatura, por sobre otras como infanto-juvenil o niños, niñas y adolescentes) y finalmente los delitos contra la propiedad intelectual y derechos afines (Título 4), que también podrían ser catalogados delictivos por su contenido, aunque el Convenio siga otra línea.

Si consideramos lo anterior, la legislación chilena sobre ciberdelitos no se circunscribe únicamente a la Ley Nº 21.459, sino que está dispersa en otros cuerpos normativos, incluyendo al Código Penal y leyes de distinta naturaleza. En el caso del Código, el legislador chileno no ha incorporado títulos especiales en torno a ciberdelitos, delitos informáticos o siquiera delitos computacionales[38], usando una técnica legislativa centrada en el objeto de protección más que en los medios o formas de ataque. Los que pudiéramos considerar como ciberdelitos se encuentran dispersados en distintos niveles y títulos.

Si lo vinculamos al Convenio, el Código contempla los recién reformados delitos de material pornográfico y de explotación sexual de niños, niñas y adolescentes (NNA), los que consideran la producción, difusión (en sentido amplio) y almacenamiento de material de esta índole, tipificados en el art. 367 quáter. Estos delitos contemplan implícitamente la utilización de tecnologías informáticas respecto al soporte del material, pues se usa la expresión "cualquiera sea su soporte", en el inciso primero. De la misma forma, consideran la utilización de redes, en particular para la comisión de buena parte de las acciones típicas del inciso primero (difundir, exhibir, comercializar, etc.), salvo para distribuir, que sería la única conducta imposible de realizar a través de redes telemáticas, por exigir soporte físico.

La misma reforma introdujo otro delito que entra perfectamente en la categoría de ciberdelitos: Se trata del tipo penal que contempla el fenómeno denominado *camming*, en el art. 367 septies, en términos de castigar la transmisión de acciones sexuales o acciones de significación sexual realizadas por menores de 18 años. De manera similar, en el sentido de intentar captar un fenómeno sexual del ciberespacio que afecta a NNA, el legislador incorporó en el art. 366 quáter una parte del *cibergrooming*, también conocido como *childgrooming*[39].

---

[38] No debemos olvidar que el Código Penal chileno fue promulgado en el año 1874, entrando en vigor un año después, siendo uno de los más longevos a nivel mundial, no obstante sus múltiples modificaciones a la fecha.

[39] Aquí, en el año 2010, a través de la Ley N° 20.526, el legislador chileno incorporó una cláusula para salvar el aparente problema de la comisión de estas conductas a distancia, por redes telemáticas, pero con una redac-

Donde también hay espacios para hablar de ciberdelitos es en el ámbito de los delitos contra la intimidad y en su convergencia con los llamados "delitos de género". En su intención por reforzar la vida privada de las personas, en el año 1995 se introdujeron al Código dos delitos contra la intimidad, que permitían el castigo a la intromisión en espacios de la vida íntima y personal, el registro o captación de imágenes, hechos, etc., y su posterior difusión, en los artículos 161-A y 161-B. Casi 15 años después, se reforzó esa protección, pero ampliando las circunstancias de lugar, con la inclusión del art. 161-C, que intenta captar penalmente el fenómeno del *upskirting*[40]. Esto se produjo a través de la Ley N° 21.153, de 2019, castiga ciertas formas de acoso sexual, siendo aquel una de sus manifestaciones[41].

Por último, y en este derrotero de normas sobre "intimidad", el legislador chileno intenta captar otro ciberfenómeno de corte sexual en el Código: El *pornrevenge* o pornovenganza[42]. Esto lo hace en el art. 161-D, incorporado por la Ley N° 21.675, del año 2024, que estatuye medidas para prevenir, sancionar y erradicar la violencia contra las mujeres, en razón de su género. La pornovenganza, más allá de las discusiones sobre su nomenclatura, es un fenómeno que afecta principalmente a mujeres, que ven como material íntimo captado por sus exparejas, de forma consentida, es difundido por redes telemáticas sin su consentimiento como una forma de castigo por el rompimiento.

Este panorama, exclusivo del Código Penal, puede complementarse con diversas leyes que consideran delitos cuya forma comisiva, implícita o explícitamente, consideran a Internet u otras redes informáticas o telemáticas, como por ejemplo la Ley N° 17.336, de Propiedad Intelectual, o la Ley N° 19.309, sobre Propiedad Industrial.

4.3 Los Delitos Informáticos Actualmente Vigentes en la Legislación Chilena

La Ley Nº 21.459 es, de forma evidente, más nutrida que su antecesora de 1993, pues además de considerar ocho tipos penales básicos y algunas figuras agravadas, agrega un articulado destinado a cuestiones procedimentales, medidas investigativas, un aparato conceptual y circunstancias modificatorias de la responsabilidad penal. Por supuesto, existen adaptaciones de otros cuerpos normativos a esta ley.

---

ción muy desafortunada. Agregó en el entonces inciso 4° (hoy inciso 5°) la expresión "mediante cualquier medio electrónico", concepto desfasado en el tiempo y que no responde a las características de las tecnologías informáticas o telemáticas, y que captan a estas solo a través de un ejercicio de interpretación progresiva, siempre amenazante del principio de legalidad. SCHEECHLER CORONA, Christian, "¿Es el tipo penal del art. 366 quáter un delito de corrupción de menores?" *en* MAYER, Laura, OLIVER, Guillermo, VERA, Jaime, org., *Hacia un derecho penal centrado en la persona. Libro homenaje al profesor Luis Rodríguez Collao*, Santiago de Chile, Editorial Jurídica de Chile, 2023, pp. 655-672.

40 Es el fenómeno consistente en captar imágenes bajo las faldas o ropa de otras personas, preferentemente niñas y adolescentes.

41 Entendida como una forma de violencia digital. HALL, Matthew, HEARN, Jeff, LEWIS, Ruth, *Digital gender-sexual violations. Violence, technologies, motivations*, New York, Editorial Routledge, 2023, pp. 17 y ss.

42 RODRÍGUEZ COLLAO, Luis, ALVARADO URÍZAR, Agustina, "Abuso sexual basado en imágenes: Un excurso necesario" *en* GONZÁLEZ JARA, Manuel Ángel, org., *Delitos sexuales*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023, pp. 13-34.

En principio, sus ocho primeros artículos son los que contienen los delitos respectivos, contándose en estos a los ataques a la integridad de los sistemas informáticos (art. 1); el acceso ilícito a dichos sistemas (art. 2); la interceptación y captación ilícitas de datos informáticos (art. 3); el sabotaje informático (art. 4); la falsificación informática (art. 5); la receptación de datos informáticos (art. 6); el fraude informático (art. 7) y el abuso de dispositivos (art. 8).

Como anticipábamos, el catálogo de ciberdelitos no se ocupó de materias tan sensibles como el tráfico de pornografía de NNA en Internet, o el uso de esta para otras formas de explotación sexual de dichos menores (como las que se incorporaron en el ya visto art. 367 del Código)[43], incluyendo la trata de seres humanos (que aunque tipificada, el legislador no le asigna un desvalor particular si se usan redes), la violencia de género digital (difusamente captada en nuestra legislación), u otros fenómenos como las "funas" o los *deepfake*.

Tampoco consideró otras figuras que pueden revestir el carácter de ciberdelitos, como aquellos relativos a contenidos de propiedad intelectual, industrial, derechos derivados o conexos, que se mantienen en leyes independientes, como se ha visto *infra*, cuyo objeto de protección forma parte del entramado artístico-comercial en una sociedad[44].

Donde sí existen referencias directas al ciberespacio como lugar de comisión de delitos es en la investigación de tales infracciones, cuyo origen también se puede encontrar en el Convenio de Budapest. El legislador refuerza la vigilancia de las comunicaciones, con el fin de obtener de cada diligencia una prueba tecnológica, pero manteniendo los debidos resguardos con la intimidad u otros derechos fundamentales de las personas que pudiesen verse afectados.

En concreto, la ley incorpora como medidas intrusivas la interceptación de comunicaciones, en el art. 12, en la medida que sea imprescindible para el éxito de la investigación, y que existan fundadas sospechas de la participación en el hecho del investigado[45]; otras técnicas de investigación, como la grabación, fotografía o la reproducción por otros medios, así como la grabación de comunicaciones entre personas presentes (interceptaciones ambientales); y muy particularmente el

---

43 GONZÁLEZ JARA, Manuel Ángel, *Corrupción, prostitución y explotación sexual en el código penal chileno*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023.

44 Esta característica, entre otras, valieron para que se introdujeran los delitos informáticos de la Ley 21.459 al catálogo de figuras que permite atribuir, bajo la Ley N° 20.393, responsabilidad penal a las personas jurídicas. MAYER, Laura, VERA, Jaime, *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*, Montevideo-Buenos Aires, Editorial IBdeF, 2024, pp. 148-149. En la misma línea, es necesario señalar que la también muy reciente Ley de Delitos Económicos, N° 21.595, del año 2024, reafirma tal cuestión, al considerar a los delitos informáticos de la Ley N° 21.459 como delitos económicos de segunda categoría, es decir, aquellos que se consideran como tales siempre que el hecho constitutivo del delito fuere perpetrado en ejercicio de un cargo, función o posición en una empresa, o cuando lo fuere en beneficio económico o de otra naturaleza para una empresa, según dispone el artículo 2 de dicha ley.

45 Vinculadas además con las normas correspondientes del Código Procesal Penal. CONTRERAS, Roberto, ARIAS, Fernando, CONTRERAS, Roberto, "Desafíos regulativos en materia de neuroderechos y ciberdelincuencia" *en* FUENTEALBA SEPÚLVEDA, Valeska, org., *Problemas contemporáneos de las ciencias penales*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023, pp. 289-304, pp. 295-297.

denominado “agente encubierto en línea”, que comprende el actuar únicamente de agentes policiales con una identidad distinta a la propia[46].

Estos aspectos procesales se transforman en un aporte relevante en materia de ciberseguridad, al entregar al poder público el equivalente a las herramientas investigativas del mundo físico, pero en el ciberespacio.

5 ACTUALIDAD Y CONTEXTO NORMATIVO DE CIBERSEGURIDAD EN CHILE

Conscientes que tanto el desarrollo del ciberespacio no admite fronteras, parte de la comunidad internacional se ha abocado a regular los diferentes ámbitos que se vinculan al ciberespacio, como es el caso de la Unión Europea. La UE ha recorrido con convicción el camino que propende a una navegación segura, abordándolo desde diferentes dimensiones.

En la década del noventa Chile tenía un nivel medio de madurez en ciberseguridad en el escenario internacional y se enfrentaba al gran desafío de contar con un ciberespacio libre, abierto, seguro y resiliente. Hasta el 2022, el marco legal y reglamentario de Chile en materia de ciberseguridad era reducido, estaba compuesto por la ya mencionada Ley Nº 19.223, la ley Nº 19.628, sobre protección de la vida privada, y la Política Nacional de Ciberseguridad 2017-2022[47].

La relevancia de contar con un ecosistema digital ha llevado a Chile a desarrollar una estrategia institucional sostenida en una triada normativa que aborda diferentes líneas de acción, y que se ha materializado en la reciente publicación de la ley N° 21.459, sobre delitos informáticos, la Ley N° 21.663, ley Marco de Ciberseguridad, y la Ley N° 21.719, sobre protección y tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Tras la revisión de la ley de delitos informáticos, revisaremos las dos últimas, recientemente incorporadas al ordenamiento nacional.

La Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información, Ley N° 21.663, es la primera en la materia en Chile y llegó a sumarse a la Política Nacional de Ciberseguridad (2023- 2028) y a la Ley de Delitos Informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes en el ciberespacio. Para ello, se dispone la creación de una institucionalidad a cargo de regular y coordinar las acciones de ciberseguridad para preservar la confidencialidad e integridad de la información y la disponibilidad y resiliencia de las redes y sistemas informáticos, además de establecer los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado, así como entre esos organismos y los particulares. De esta forma, la creación de la Agencia Nacional de Ciberseguridad (art.10) es un primer paso esencial para comenzar a construir una política pública en estas materias.

---

46 ALVARADO URÍZAR, Agustina, “Diligencias intrusivas en la nueva ley de delitos informáticos. Análisis crítico” *en* SCHEECHLER CORONA, Christian, org., *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones, 2021, pp. 257-296, pp. 268 y ss.

47 Política Nacional de Ciberseguridad 2017-2022, del Ministerio del Interior y Seguridad Pública de Chile.

El nuevo Marco provee una estructura regulatoria aplicable a instituciones del sector público y privado que posean infraestructura crítica de información y que califiquen -de acuerdo de acuerdos a los criterios definidos en la ley- como "prestadores de servicios esenciales" u "operadores de importancia vital". Para dichas instituciones se establecen deberes específicos, como implementar un sistema de gestión de riesgo permanente y planes de continuidad operacional y de ciberseguridad.

Asimismo, consagra la creación de un Equipo Nacional de Respuesta ante Incidentes de Seguridad Informática (CSIRT Nacional) (art. 24), de Equipos Sectoriales de Respuesta ante Incidentes de Seguridad Informática (CSIRT Sectorial) (art.27), y un Comité Interministerial de Ciberseguridad (art.48).

Otra de las importantes contribuciones de esta ley, es el establecimiento de infracciones y sanciones (art.38) que podrán ser cursadas por la Agencia Nacional de Ciberseguridad, cuando se incurra en algunas de las conductas que la referida ley establece. Indudablemente, el establecimiento de multas con elevada cuantía tiene una finalidad disuasoria y pretenden elevar los estándares de ciberseguridad. Así, por ejemplo, el art. 40° establece que la multa podrá alcanzar las 40.000 Unidades Tributarias Mensuales[48] (en adelante "UTM"), en caso de que el infractor sea un operador de importancia vital.

En la configuración del tejido normativo de ciberseguridad en Chile, un abordaje solo desde la seguridad de la información no resulta suficiente y se requiere una perspectiva amplia que pondere a la ciberseguridad como un derecho digital y como un vehículo para el resguardo de bienes jurídicos. De esta manera, un ciberespacio libre y seguro depende de un ecosistema institucional multidisciplinar que coordine las diferentes aristas que se relacionan con el ciberespacio.

En este escenario, la protección de datos es fundamental para resguardar la integridad de la información. Desde 1999, Chile contaba con la Ley N° 19.628, sobre Protección de la Vida Privada, siendo pioneros en Latinoamérica en una época en la que aún no se masificaba la participación en el espacio virtual. Sin embargo, con el desarrollo de las nuevas tecnologías informáticas y telemáticas, la normativa en cuestión fue perdiendo vigencia, tal como ocurrió con la Ley Nº 19.223, de delitos informáticos. En el año 2018, mediante la Ley Nº 21.096, los datos personales se consagraron como un derecho fundamental en la Constitución Política; sin embargo, las garantías constitucionales previstas no son suficientes para la tutela efectiva de este derecho constitucional, recordándonos el tradicional aforismo jurídico "Ubi jus, ibi remedium", que se traduce como "Donde hay un derecho, hay un remedio", es decir, para su pleno ejercicio los derechos deben contar con herramientas que permitan su exigibilidad.

Así, continuando la senda trazada por el Reglamento General de Protección de Datos de la Unión Europea[49], que constituye una referencia internacional para la

---

[48] A saber, 40.000 Unidades Tributarias Mensuales equivalen a $2.691.760.000 (pesos chilenos), equivalentes a 2.600.744,3 (euros).

[49] PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, "Reglamento (UE) 2016/679 de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", Estrasburgo, Unión Europea, 2016, Disponible en: https://eur-lex.europa.eu/, Acceso en: 30 dic. 2024.

protección de los derechos de las personas y sus datos personales, Chile publicó una nueva Ley de Protección y Tratamiento de Datos Personales, N° 21.719[50], elevando el estándar de protección a los derechos de las personas mediante la actualización del marco normativo para su tratamiento.

El nuevo cuadro de protección de datos, en el art.2 incorpora principios para las operaciones sobre datos (licitud y lealtad, finalidad, proporcionalidad, calidad, responsabilidad proactiva, transparencia e información y confidencialidad), aumenta las exigencias para el responsable del tratamiento, quién deberá adoptar las medidas pertinentes para generar el cambio cultural que les permita actuar en conformidad.

La Ley N° 21.719 introduce un sólido enfoque preventivo a través de importantes cambios en la institucionalidad, como la creación de la Agencia de Protección de Datos (con facultades sancionatorias) (art.30) y del delegado de Protección de Datos (art.50). Además, establece un modelo preventivo de infracciones (art.49) y un régimen sancionatorio para las empresas que incumplan la normativa, y subsana la omisión de la protección de datos de los menores que adolecía la Ley Nº 19.628, considerándolos como datos de especial protección, en sintonía con la preocupación plasmada en la Ley de Delitos Informáticos.

En este contexto, la ciberseguridad se ha consolidado como un pilar fundamental del espacio virtual, lo que ha llevado a los Estados a adoptar estrategias alineadas con estándares internacionales y a suscribir acuerdos de cooperación global[51]. Empero, dado que la comunidad internacional enfrenta desafíos significativos para avanzar de manera uniforme en el desarrollo normativo, el *soft law* emerge como una alternativa viable para fomentar el progreso. Un ejemplo reciente de ello es la suscripción de la Carta Iberoamericana de Derechos Digitales (2023), que sigue la línea de la Declaración Europea sobre Derechos y Principios Digitales (2022) y la Carta de Derechos Digitales de España (2021). Esta última iniciativa logró posicionar a España como un referente en el reconocimiento de derechos digitales en el ciberespacio, promoviendo un marco normativo más inclusivo y adaptado a la era digital.

Los desafíos que enfrenta la ciberseguridad reflejan la necesidad de una constante actualización normativa y evolución de políticas públicas para responder los riesgos del entorno digital. Desde la perspectiva regulatoria, urge un enfoque integrador capaz de coordinar la institucionalidad y sistematizar la normativa fragmentada, así como también enfatizar en los valores jurídicos y derechos fundamentales que dependen de la ciberseguridad, mediante políticas públicas de prevención, sanción y concientización. Desde la criminología y derecho penal, es menester abordar los nuevos fenómenos delictivos en el ciberespacio y el surgimiento de nuevas figuras delictuales provenientes de la convergencia tecnológica.

---

[50] Ley N° 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, del Ministerio Secretaría General de la Presidencia. Publicada en el Diario Oficial el 13 de diciembre de 2024, y entrará en vigor el 01 de diciembre de 2026.

[51] Véase CORTÉS CABRERA, Bárbara, "Ciberseguridad en la Unión Europea y su influencia en la nueva ley de delitos informáticos" *en* SCHEECHLER CORONA, Christian, org., *Los delitos informáticos. Aspectos políticos-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones, 2024, p. 61.

6 CONCLUSIONES

En un Estado constitucional y democrático de Derecho, la seguridad es un elemento indispensable para el desarrollo y bienestar social de la ciudadanía y donde los derechos fundamentales son su eje. En la dimensión del ciberespacio, esto se traduce en el rol preponderante del Estado de proveer y garantizar un ciberespacio libre y seguro, así como velar por el respeto y protección de los derechos fundamentales en la Red y mantener la fiabilidad e interoperabilidad de Internet.

Chile ha demostrado avances notables en materia de regulación de la actividad en el ciberespacio, especialmente con la promulgación de nuevas leyes, como aquella sobre delitos informáticos, la Ley Marco de Ciberseguridad e Infraestructura Crítica de Información, y la Ley sobre protección de datos personales. Estas iniciativas reflejan el compromiso del legislador por modernizar el marco legal y adaptarlo a los desafíos de un ciberespacio dinámico y transformador.

Sin embargo, persisten importantes retos normativos y operativos, tales como la necesidad de enfrentar fenómenos emergentes, como los *deepfakes*, el tráfico de pornografía de NNA en internet, la violencia de género digital y el uso indebido de tecnologías avanzadas como la inteligencia artificial. Estos desafíos reflejan la naturaleza del ciberespacio y la necesidad de ampliar y sistematizar la normativa e institucionalidad, junto con promover la cooperación internacional y responder conforme a los estándares internacionales.

De esta manera, el modelo implementado por la Unión Europea constituye un referente importante para Chile, ya que el ciberespacio, por su naturaleza transfronteriza, requiere directrices multidisciplinarias y de cooperación internacional. Este aspecto es fundamental para abordar problemáticas como la persecución de ciberdelitos y la atribución de responsabilidades. Chile enfrenta el desafío de darle curso a una esperada institucionalidad que sea capaz de anticiparse a las amenazas y responder de manera ágil, para garantizar un ciberespacio libre y seguro, con políticas públicas que equilibren el desarrollo tecnológico, la seguridad de las infraestructuras críticas y la protección de los derechos fundamentales.

7 REFERENCIAS

AGUILAR CÁRCELES, Marta, "Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido", *Revista Cuadernos de Política Criminal*, n. 110, 2013, pp. 221-259.

ALVARADO URÍZAR, Agustina, "Diligencias intrusivas en la nueva ley de delitos informáticos. Análisis crítico" *en* SCHEECHLER CORONA, Christian, org., *Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones, 2021.

ÁLVAREZ ROBLES, Tamara, *El Derecho de acceso a Internet. Especial referencia al Constitucionalismo español*, Valencia, Editorial Tirant Lo Blanch, 2024.

ASOCIACIÓN POR LOS DERECHOS CIVILES, *Descubriendo la agenda de ciberseguridad de Latinoamérica: el caso de Argentina, ¿Qué entendemos por ciberseguridad?*, primera entrega, Ottawa, Cyber Stewards Network, 2015, Disponible en: <https://adc.org.ar/wp-content/uploads/2019/06/007-A-descubriendo-la-agenda-de-ciberseguridad-de-america-latina-el-caso-argentina-1ra-entrega-10-2015.pdf>, Acceso en: 30 dic. 2024.

BARRIO ANDRÉS, Moisés, *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*, Valencia, Editorial Tirant Lo Blanch, 2018.

BEQUAI, August, *Computer crime,* Lexington, Editorial Health Lexington Books, 1978, Crimen informático.

BLAS ZULUETA, Luis, "Delitos informáticos", *Revista General de Derecho*, n. 495, 1985, pp. 310 – 311.

BOLAÑOS RAMÍREZ, M.R., "El delito informático como nueva figura jurídica", *en* AAVV, org., *Actas del Primer Congreso Iberoamericano de Informática Jurídica*, Madrid, Editorial CREI, 1985.

CAMACHO LOSA, Luis, *El delito informático*, Madrid, Editorial Gráficas Cóndor, 1987.

CANALS AMETLER, Dolors, *Ciberseguridad. Un nuevo reto para el Estado y los Gobiernos Locales*, primera edición, Madrid, Editorial El Consultor De Los Ayuntamientos, 2021.

CASTELLS OLIVÁN, Manuel, "Globalización, Estado y sociedad civil: El nuevo contexto histórico de los derechos humanos", *Revista Isegoría*, n. 22, 2000, pp. 5-17.

CONTRERAS, Roberto, ARIAS, Fernando, CONTRERAS, Roberto, "Desafíos regulativos en materia de neuro-derechos y ciberdelincuencia" *en* FUENTEALBA SEPÚLVEDA, Valeska, org., *Problemas contemporáneos de las ciencias penales*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023.

CORTÉS CABRERA, Bárbara, "Ciberseguridad en la Unión Europea y su influencia en la nueva ley de delitos informáticos" *en* SCHEECHLER CORONA, Christian, org., *Los delitos informáticos. Aspectos políticos-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones, 2024.

CRUZ DE PABLO, José, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, Madrid, Editorial Grupo Difusión, 2006.

DOMÍNGUEZ ÁLVAREZ, José Luis, "Derecho a la seguridad digital: génesis, evolución y perspectivas de futuro" *en* RODRÍGUEZ AYUSO, Juan, org., *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, Navarra, Editorial Thomson Reuters Aranzadi, 2022.

FABA DE LA ENCARNACIÓN, Elena, SIMON CANAL, Tomás, "Soberanía digital: ¿Un problema normativo o un problema geopolítico?", *Revista de Economía Industrial: Soberanía Tecnológica e Industrial*, n.427, 2023, pp. 45-47.

GONZÁLEZ JARA, Manuel Ángel, *Corrupción, prostitución y explotación sexual en el código penal chileno*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023.

GUTIÉRREZ FRANCES, María Luz, *Fraude informático y estafa (aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos),* Madrid, Editorial Ministerio de Justicia, Secretaría General Técnica, Centro de Publicaciones, 1991.

HALL, Matthew, HEARN, Jeff, LEWIS, Ruth, *Digital gender-sexual violations. Violence, technologies, motivations*, New York, Editorial Routledge, 2023.

IBÁÑEZ MUÑOZ, Josep, "Globalización e Internet: poder y gobernanza en la sociedad de la información", *Revista Relaciones Internacionales*, n.4, 2006, pp. 1 -33.

LUZÓN PEÑA, Diego, *Enciclopedia penal básica,* Granada, Editorial Comares, 2002.

MATA Y MARTÍN, Ricardo, *Delincuencia informática y derecho penal*, Madrid, Editorial Edisofer, 2001.

MAYER LUX, Laura, "El cibercrimen en tiempos de la nueva ley de delitos informáticos" en SCHEECHLER CORONA, Christian, org*., Los delitos informáticos. Aspectos político-criminales, penales y procesales en la Ley N° 21.459*, Santiago de Chile, Editorial DER Ediciones.

MAYER, Laura, VERA, Jaime, *Delitos informáticos y cibercriminalidad. Aspectos sustantivos y procesales*, Montevideo-Buenos Aires, Editorial IBdeF, 2024.

MUÑOZ MACHADO, Santiago, *La regulación de la Red. Poder y Derecho en Internet*, Madrid, Editorial Taurus, 2000.

ORGANIZACIÓN DE ESTADOS AMERICANOS, *Reunión de Expertos en el Ciberdelito*, 2003, Disponible en: <https://www.oas.org/es/>, Acceso en: 30 dic. 2024.

OXFORD DICTIONARIES, *Oxford Languages,* Disponible en: <http://www.oxforddictionaries.com/es/traducir/ingles-espanol/computer>, Acceso en: 29 dic. 2024.

PARLAMENTO EUROPEO, CONSEJO DE LA UNIÓN EUROPEA, "Artículo 2" en Parlamento Europeo y del Consejo, org., *Reglamento (UE) 2019/881 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) Nº 526/2013 (Reglamento sobre la Ciberseguridad)*, Estrasburgo, Unión Europea, 2019, Disponible en: <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019R0881>, Acceso en: 30 dic. 2024.

PÉREZ BES, Francisco, *Memento experto ciberseguridad*, Madrid, Editorial Francis Lefebvre, 2021.

REAL ACADEMIA DE LA LENGUA ESPAÑOLA, *Ciberespacio. Diccionario de la Lengua Española,* Edición del Tricentenario, Disponible en: https://dle.rae.es/ciberespacio?m=form, Acceso en: 30 dic. 2024.

RODRÍGUEZ COLLAO, Luis, ALVARADO URÍZAR, Agustina, "Abuso sexual basado en imágenes: Un excurso necesario" *en* GONZÁLEZ JARA, Manuel Ángel, org., *Delitos sexuales*, Santiago de Chile, Ediciones Jurídicas de Santiago, 2023.

ROMEO CASABONA, Carlos, "De los delitos informáticos al cibrecrimen. Una aproximación conceptual y político-criminal" *en* ROMEO CASABONA, Carlos, org., *El Cibercrimen. Nuevos retos jurídicos-penales, nuevas respuestas político-criminales*, Granada, Editorial Granada Comares, 2006.

ROMEO CASABONA, Carlos, *Poder informático y seguridad jurídica,* Madrid, Editorial Fundesco, 1987.

ROVIRA DEL CANTO, Enrique, *Delincuencia informática y fraudes informáticos*, Granada, Editorial Comares, 2002.

SCHEECHLER CORONA, Christian, "¿Es el tipo penal del art. 366 quáter un delito de corrupción de menores?" *en* MAYER, Laura, OLIVER, Guillermo, VERA, Jaime, org., *Hacia un derecho penal centrado en la persona. Libro homenaje al profesor Luis Rodríguez Collao*, Santiago de Chile, Editorial Jurídica de Chile, 2023.

SIEBER, Ulrich, "Criminalidad informática: peligro y prevención" *en* MIR PUIG, Santiago, org., *Delincuencia informática*, Barcelona, Editorial Promociones y Publicaciones Universitarias, 1992.

SIEBER, Ulrich, "Documentación para una aproximación al delito informático" *en* MIR PUIG, Santiago, org., *Delincuencia informática*, Barcelona, Editorial Promociones y Publicaciones Universitarias, 1992.

SIEBER, Ulrich, *The International Handbook on Computer Crime: Computer-related Economic Crime and the Infringements of Privacy*, Michigan, Editorial Wiley, 1986, Manual internacional sobre delitos informáticos: delitos económicos relacionados con la informática y violaciones de privacidad.

SMITH, Russell, GRABOSKY, Peter, URBAS, Gregor, *Cyber criminals on trial*, Cambridge, Editorial University Press, 2004.

TORTRAS Y BOSCH, Carlos, "El delito informático", *Revista Informática y Derecho,* n. 17, 1989, pp. 45-50.