Universidad de Chile
Facultad de Derecho
Departamento de Ciencias Penales

LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS Y SU PRUEBA EN MATERIA PENAL

MEMORIA PARA OPTAR AL GRADO DE LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

ESTUDIANTE: ABDI CORNEJO CONTRERAS

PROFESOR GUÍA:
ERNESTO VÁSQUEZ BARRIGA

SANTIAGO DE CHILE
2023

AGRADECIMIENTOS

Agradezco a DIOS en primer lugar, por ser el TODO de mi vida. El cual me ha acompañado a transitar este difícil camino, y me permite estar donde me encuentro hoy;

a mamá, que ha sido la mejor madre del mundo que DIOS me pudo dar, y que espero no me falte nunca, le agradezco por ser mi motor y mi motivación, la persona que me acompaña en mis tristezas y alegrías;

y a mi mejor amigo, al cual siempre amaré,
que fue papá, hoy en memoria de él.

“Porque Jehová da la sabiduría,
Y de su boca viene el conocimiento y la inteligencia.
Él provee de sana sabiduría a los rectos;
Es escudo a los que caminan rectamente.
Es el que guarda las veredas del juicio,
Y preserva el camino de sus santos.
Entonces entenderás justicia, juicio
Y equidad, y todo buen camino.”

-Proverbios 2:6-9

TABLA DE CONTENIDO

I. RESUMEN

La presente investigación tiene por objeto desglosar con mayor detalle el rol policial en la investigación de los delitos informáticos, que en la actualidad ha ganado una expansión notable en la sociedad debido a los sucesos acontecidos, como lo es a modo de ejemplo la pandemia del virus SARS-CoV-2, lo que ha hecho que en pleno siglo XXI, el ciberespacio sea utilizado con notable frecuencia por las personas.

Se aborda con respecto a este tópico, haciendo una síntesis de la historia del delito informático, detallando el tratado internacional ratificado y suscrito por Chile en materia de ciberseguridad, asimismo se enfoca en la legislación chilena en torno a la tipicidad de las figuras delictivas con relación al delito informático, como también se pronuncia en el presente análisis acerca de los delitos informáticos *in situ*, características, *modus operandi,* expansión a nivel global, como legislación en torno a perseguir estos delitos. De igual forma se abordan las potestades y atribuciones de las policías en torno a la persecución e investigación de estos delitos, así como la capacidad técnica para investigar.

De este modo, con la presente memoria se quiere contribuir a diagnosticar posibles respuestas a la legislación chilena acorde al problema que nos confiere en el presente y a futuro, los delitos informáticos y de ciberseguridad en lo que se refiere a los requerimientos que la sociedad requiere en torno a la parte investigativa de las policías, como de igual manera hacer presente que es necesario acomodar la normativa actual a las exigencias del Convenio sobre la Ciberdelincuencia del Consejo de Europa, comúnmente denominado *"Convenio de Budapest"* , el cual Chile ha suscrito y ratificado.

II. INTRODUCCIÓN

El avance de la tecnología provocó durante la última década avances agigantados. Se ha intensificado el acceso a internet en nuestro país, logrando que sea la nación con mayor proporción de conexiones a internet a escala de países Latinoamericanos[1].

En Chile, la ley 19.223, de larga data, fue un avance plausible para el periodo en el cual se promulgó, respectivamente, el año 1993. Eso sí, solamente penalizaba el sabotaje o espionaje informático con penas de 61 días a 3 años de cárcel, que para la época en que se confeccionó constituyó, en efecto, un avance. Sin embargo, al año presente ya era posible clasificarla como una ley obsoleta de acuerdo a cómo ha avanzado el delito informático.

La ley 21.459 establece una mayor cantidad de normas para los delitos informáticos, con el fin de adecuar nuestra legislación al convenio internacional suscrito y ratificado por Chile, denominado comúnmente *"Convenio de Budapest"*. Dicho lo anterior, reside entonces en la nueva ley 21.459, promulgada el 20 de Junio de 2022, una ardua misión consistente en reemplazar y mejorar a la derogada ley 19.223. Dentro de los objetivos relevantes que se plantea, se pretende tipificar delitos informáticos y realizar su persecución de manera eficiente. Anhela la realización de una correcta investigación policial en los delitos informáticos, a fin de obtener una suficiente como fidedigna prueba en materia penal. Con esto se busca lograr mayor alcance y poder para combatir un nuevo fenómeno que ha tomado cada vez más fuerza en el siglo 21, como lo es, la ciberdelincuencia, otorgando de este modo, como fin superior, una mayor seguridad a la ciudadanía nacional con respecto a este tópico, en pleno desarrollo del siglo XXI.

En lo relativo al rol que cumplen las policías en la investigación de los delitos informáticos y su prueba en materia penal, es un tema complejo, dado que las investigaciones penales con relación a los delitos informáticos en la actualidad, se pueden transformar en crisoles laberínticos y dificultosos.

[1] NAVEDA, J. (2021). C*hile es el país con mayor proporción de conexiones a internet de Latinoamérica.* Comscore. Consultado el 2 de Noviembre de 2022. Recuperado de: https://www.comscore.com/lat/Prensa-y-Eventos/Blog/Chile-es-el-pais-con-mayor-proporcion-de-conexiones-a-Internet-de-Latinoamerica#:~:text=Chile%20es%20el%20pa%C3%ADs%20latinoamericano,76%25%20de%20la%20poblaci%C3%B3n%20total.

En efecto, existen comportamientos que pueden ser difíciles de encasillar dentro de tres grupos de hipótesis, esto es, sabotaje informático, espionaje informático o fraude informático[2]. Principalmente, porque pueden llevarse a cabo para posibilitar o facilitar la ejecución de otras conductas que integran la criminalidad informática. Esto ocurre, a modo de ejemplo, con la difusión de *malware* o *software* malicioso, o con el acceso indebido a datos o programas informáticos, que es comúnmente conocido como *hacking*[3], que pueden orientarse a la ejecución de un delito dentro de los tres grupos mencionados más arriba.

Ahora bien, cabe mencionar que los delitos informáticos son transnacionales[4], es decir, no conocen de fronteras. Con esa información, además de tener conocimiento de que actualmente se está ocasionando una masificación sorprendente del uso de internet y la creación de dispositivos electrónicos cada vez más fáciles de utilizar, como de adquirir, Chile suscribió el "*Convenio de Budapest*", el primer tratado internacional creado para enfrentar los delitos informáticos de manera global, en conjunto con diversos países[5].

En fin, tanto la experiencia comparada como también en la local, con el correr del tiempo, ha expuesto que el avance tecnológico trae consigo también nuevos peligros, nuevas formas de ataque contra bienes jurídicos relevantes. Frente a lo cual, surge especialmente la pregunta por la capacidad de reacción de los tipos penales tradicionales frente a formas de criminalidad desarrolladas al alero del desarrollo informático, en especial se pone énfasis sobre la investigación del delito informático y la prueba, como también, se pone en cuestión el qué tan preparada se encuentra la sociedad civil, las policías y el ministerio público para hacer

---

[2] MAYER LUX, L. (2018) *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos.* Scielo. Consultado el 4 de Noviembre de 2022. Recuperado de https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext#:~:text=La%20criminalidad%20inform%C3%A1tica%20se%20caracteriza,%E2%80%9Cglobalizaci%C3%B3n%20del%20delito%E2%80%9D57.

[3] En un inicio, tal comportamiento se entendió de dos perspectivas diversas entre sí: de un lado, comomero acceso a datos o programas de terceros, que se le conoce como hacking puro o blanco (por todos Galán [2009], Pág. 94); por otro lado, como acceso indebido (Sieber (2014), Pág. 437) a datos o programas con intención de dañar a terceros, supuesto que recae dentro de la noción en lo que concierne a cracking (Moscoso (2014), Pág. 33). Con el tiempo se ha ido imponiendo la de que "la intromisión en sistemas ajenos no tiene cabida, cuanto menos en el marco de la legalidad" y que "todo "Hacking es cracking" (Miró (2012). Pág. 56, quien también alude a las consecuencias negativas que puede tener la tendencia a equiparar el hacking y el cracking).

[4] MAYER LUX, L. (2018) Op. Cit.

[5] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia del Decreto Supremo Nº 83. Aprueba el Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre 2001*. Consultado el 19 de Diciembre de 2022. Recuperado de: https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/6527/#:~:text=El%20Convenio%20sobre%20la%20Ciberdelincuencia%20del%20Consejo%20de%20Europa%2C%20conocido,y%20de%20otros%20sistemas%20inform%C3%A1ticos.

frente a los delitos informáticos, cuestión que se expondrá con mayor extensión en los siguientes capítulos. Se hace énfasis y recalca que se adoptará un orden partiendo **desde lo más amplio del delito informático, hasta llegar a lo más específico** que sería lo relacionado a la investigación y prueba en materia penal en torno al delito informático. Para poder comprender de mejor manera el delito informático se detallan cómo surgieron los delitos informáticos, definiciones, la normativa vigente en Chile con los tratados suscritos y ratificados por esta nación, las políticas adoptadas por el país en torno al tema, análisis individual y comparativos, desafíos en torno al tema, dado que para entender la investigación y recopilación de prueba es necesario conocer que significa todo lo anterior, con el objetivo de entregar un completo trabajo sobre esta materia.

III. Capítulo 1. SÍNTESIS DE LA HISTORIA DEL DERECHO INFORMÁTICO Y CONCEPTO DE DELITO INFORMÁTICO

En la actualidad, tomando como referencia el año 2023, se configura dentro de un marco al cual se le ha denominado **"Sociedad de la información"**[6], la cual es aquella en donde las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas. Otra característica con respecto a esta terminología, es que el núcleo de contexto debe estar centrado en la persona, tiene que ser integradora y con una orientación al desarrollo, en donde todos puedan crear, consultar, utilizar y compartir la información como el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida[7].

Dentro de la sociedad de la información localizamos canales que hacen factible el traslado y traspaso de información de un sector a otro. En esos canales se localizan las **"Redes Sociales"**, las cuales se pueden definir como *"aquel servicio que la sociedad de la información brinda a los usuarios una plataforma de comunicación a través de internet, para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que pueden interactuar mediante mensajes, compartir información, imágenes o videos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios de su grupo"*[8]. Las redes sociales en el día de hoy han pasado a ser una base elemental en torno a la información que puede consumir una persona, ya sea en un corto tiempo y largo alcance, no importando las barreras de distancia. Para hacer esto posible no puede lograrse sino con una comunicación a nivel expansivo, lo que hizo posible la internet.

Internet surge en Estados Unidos como un proyecto militar frente a posibles ataques en contra de ese país. En el año 1969, se envió el primer mensaje host-to-host desde el laboratorio de Kleinrock en la Universidad de California en Los Ángeles. Creciendo

---

[6] BANDERAS, R (2009). *¿Sociedad de la información o sociedad del conocimiento?.* El Cotidiano. Pág.75-80.
[7] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. *Sociedad de la Información.* Consultado el 19 de Diciembre de 2022. Recuperado de: https://mintic.gov.co/portal/inicio/Glosario/S/5305:Sociedad-de-la-Informacion.
[8] REAL ACADEMIA ESPAÑOLA. *Red Social.* Recuperado de: https://dpej.rae.es/lema/red-social.

rápidamente el desarrollo en ese ámbito, otros dos nodos fueron agregados en la Universidad de California en Santa Barbara y la Universidad de Utah. Al terminar el año, las cuatro computadoras estaban conectadas en ARPANET, y con ello se creaba la internet[9]. Tenía como objetivo establecer una conexión entre el Pentágono, las universidades y grandes empresas que se dedicaban a la investigación militar de cualquier tipo. Es en el año 1986 cuando la National Science Foundation implementa en Internet una segunda arteria de comunicaciones que con cinco superordenadores conectaba todas las universidades del país, dando acceso a los alumnos de las mismas.

Al hacer un contraste en relación con su origen, tanto Internet como la mayoría de las redes informáticas, nacen en la universidad y se pueden considerar la génesis de los medios masivos para poder comunicarse: *"Las redes informáticas académicas constituyen el antecedente inmediato de las autopistas de la comunicación, siendo el núcleo universitario su lugar de nacimiento y desarrollo"*[10].

Dicho lo anterior, se puede decir que de alguna manera es la culminación de la *"... realización espacial de la utopía anarquista"*[11], en el sentido de que nadie gobierna la red, aunque existe la posibilidad de identificar al emisor de ofensas, calumnias, etc.

Por otra parte, al año 2022, con el surgimiento, expansión y uso de teléfonos inteligentes, como de artefactos tecnológicos que permiten ingresar a internet, ha generado un crecimiento exponencial cada vez más fuerte del ciberespacio[12]. Hoy la sociedad se encuentra en un estado de mayor vulnerabilidad, debido a la reducción de tamaños y costos en torno a la adquisición de dispositivos electrónicos que son medios para cometer el delito informáticos, junto con ser diseñados como dispositivos de arquitecturas abiertas y con amplia conectividad a sistemas locales, regionales e incluso internacionales, de transferencia de información de gran velocidad y compleja identificación de su punto de origen. Por esta razón se ha experimentado una disminución en los niveles de seguridad informática que presenciamos en los inicios de la informática[13].

---

[9] CSIRT. *Hitos de la historia de Internet.* Consultado el 4 de Abril de 2023. Recuperado de: https://www.csirt.gob.cl/noticias/hitos-de-la-historia-de-internet/.
[10] LÓPEZ DE ARENOSA, R. (1994). *IRIS, red informática del Plan Nacional de I + D*. Política Científica, n° 40, julio. Pág. 31-32.
[11] VERDÚ, V. (1994). *Está usted entrando en Internet*. El País Semanal, año XIX, n° 198. Pág. 70-75.
[12] CIBERSEGURIDAD. *Ciberespacio.* Consultado el 6 de Enero de 2023. Recuperado de: https://ciberseguridad.com/guias/recursos/ciberespacio/.
[13] LIBICKY M. (2000). *The future of information Security*, Institute for National Strategic Studies. Pág. 1.

Frente a los antiguos como más recientes tipos delictivos relacionados con el uso de aparatos inteligentes y la internet, aparece como contraparte en concepto de *ciberseguridad*, el cual se entiende como la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil[14].

De igual forma, en torno al derecho, la era de la información deja abierta la puerta a que criminales ocupen nuevas plataformas para llevar a cabo nuevos tipos de delitos. Es por ello que fue necesario el nacimiento de una nueva rama del derecho, la cual se le denominó "Derecho informático" o "*Rechtsinformatik".* Este concepto fue empleado por el profesor Wilhelm Steinmüller, quien en la década de 1970 en adelante, se refirió así a estas materias en la Universidad de Ratisbona (Regensburg). Otros autores le han llamado derecho telemático, derecho de las nuevas tecnologías, iuscibernética, derecho tecnológico, derecho del ciberespacio, derecho de internet, derecho de las TIC y, más recientemente, derecho digital[15].

Más allá de la denominación, lo relevante es que todos estos conceptos aluden a lo mismo, esto es, se trata de principios y de un *"conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones"*[16]*.*

Cabe acentuar, que dentro de los objetivos de aquellos dedicados a esta disciplina, ha sido analizar la aptitud del sistema normativo para regular adecuadamente la nueva realidad, tomando como referencia el análisis de las reglas generales y principios que rigen en nuestro ordenamiento jurídico, verificando si pueden ser subsumidas en sus normas las hipótesis que surgen del empleo de las Tecnologías de la Información y Comunicación[17].

---

[14] KASPERSKI. *¿Qué es la ciberseguridad?.* Consultado el 18 de Octubre de 2022. Recuperado de: center/definitions/what-is-cyber-security.
[15]DONOSO ABARCA, L. REUSSER MONSÁLVEZ, C.(2021). *Derecho Informatico*. Academia Judicial. Pág. 13.
[16] CARRASCOSA, V. (1995). *"El Derecho Informático como asignatura para juristas e informáticos"*. Revista de Informática y Derecho, Universidad Nacional de Educación a Distancia. Merida. Pág. 3.
[17] ARBALÁEZ, M. (2014). *Las tecnologías de la información y la comunicación (TIC) un instrumento para la investigación*. Consultado el 4 de Febrero de 2023. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81462014000200001.

En lo sustancial, es necesario exponer aquellos principios[18], los cuales que integran el derecho informático como disciplina jurídica, dentro de los cuales observamos:

a) Respeto a la dignidad humana como base del sistema normativo: en virtud del reconocimiento de que todo ordenamiento jurídico tiene como objetivo central la regulación de la vida humana en sociedad en el interés público.

b) Autonomía de la voluntad: El reconocimiento de la libertad humana y el respeto a la autonomía de la voluntad, tal como se refleja en la autodeterminación humana, tiene una importancia imperiosa en el derecho informático.

c) Igualdad ante la ley: Como principio fundamental, la igualdad de acceso a las redes sociales y servicios se considera un factor clave hacia una comunidad más desarrollada y justa.

d) Principio de buena fe: Tiene sus manifestaciones en las normas de derecho informático. El principio de buena fe, enunciado en el Código Civil como *"la conciencia de haber adquirido el dominio por un medio lícito, exento de fraude y de cualquier otro vicio"*[19], pero que en general podemos entender como la conciencia de un sujeto sobre la bondad, rectitud o transparencia de su proceder, tiene plena vigencia en el área que aquí nos ocupa.

e) Neutralidad tecnológica: Dentro de la cual se encuentra la equivalencia funcional y la no discriminación. Se entiende que las normas generales o específicas establecen los derechos y deberes de las personas, pero no definen los medios técnicos necesarios para cumplir los fines normativos.

Por su propia naturaleza virtual, la regulación jurídica del ciberespacio y los delitos informáticos se convierte en muchas ocasiones en fuente de conflictos. A los gobiernos les resulta difícil hacer cumplir sus leyes. Como resultado, los delitos cometidos en este entorno son difíciles de perseguir y enjuiciar. Relacionado con lo anterior, en la sociedad actual existen activistas que mantienen la independencia y autonomía del ciberespacio, exigiendo que las autoridades estatales no ejerzan control, ni ejerzan censura. Sin embargo, es de notable

[18] DONOSO ABARCA, L. REUSSER MONSÁLVEZ, C. (2021). Op. Cit. Pág 17-20.
[19] Código Civil de Chile. Artículo 706 inciso 1.

necesidad el regular el uso, abuso y administración de la información que fluye por el ciberespacio. En apoyo a lo aludido, se desarrolló el concepto de *ciber ética*, el cual se puede definir como *"aquel estudio filosófico de ética relacionado con los entornos virtuales, que abarca el comportamiento del usuario ante lo que las computadoras están programadas para hacer, y cómo esto afecta a las personas y la sociedad"*[20].

III.1 Concepto de Cibercrimen y Delito Informático

A partir de la mirada del delito propiamente tal, desde una concepción amplia, el cibercrimen puede ser definido como *"cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet"*[21].

En cambio, desde una concepción restringida, constituirá cibercrimen solamente aquel comportamiento delictivo que se realiza en el ciberespacio *"cuya esencia de injusto no podría haberse dado de ninguna forma fuera de él"*[22].

La diferencia conceptual entre cibercrimen y delito informático es, por una parte, que el **cibercrimen abarca en sentido amplio, tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución solamente es posible gracias a la existencia de dichos medios.** Y dentro de este término genérico, los delitos informáticos serían **aquellas conductas delictuales en que se atacan bienes informáticos en sí mismos, no como medio, como por ejemplo, dañar el Software mediante la intromisión de un virus**[23]**.**

[20] OLIVETTI, C. (2019). *¿Qué es la Ciberética?.* (Comentario en la página web*).* Linkedin. Consultado el 3 de Septiembre de 2022. Recuperado de: https://es.linkedin.com/pulse/qu%C3%A9-es-ciber%C3%A9tica-carmen-olivetti.
[21] MIRÓ LLINARES, F.(2012). *El Cibercrimen*. Editorial Marcial Pons. Madrid. Pág. 42.
[22] Ibidem. Pág. 42
[23] CAVADA, J. (2020). *Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera*. Biblioteca del Congreso Nacional. Pág 1. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf.

También hay quienes hacen sinónimo de “ciberdelito” o “cibercrimen”, al señalar que estos se entienden como cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito[24].

En el mismo sentido, homologando, se dice que delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet[25].

Ahondando mayormente, desde la doctrina, el concepto de delito informático, según Jijena Leiva, es bastante completo y didáctico a esbozar. Entendemos de esa forma por delito informático aquella *“acción típica, antijurídica, con intención dolosa o por negligencia, culpable, cometida contra el soporte lógico de un sistema informático o de tratamiento automatizado de información, generalmente mediante elementos computacionales”*[26].

Por otra parte, autores como Miguel Ángel Davara Rodríguez lo hacen, en términos amplios, como un conjunto de comportamientos dignos de reproche penal, que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con esta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos en alguna de sus fases de ejecución[27].

Otro sector de la doctrina, en cambio, restringe la conceptualización a aquellos ilícitos que *incluyen* los medios informáticos en alguna de las fases de ejecución de la conducta lesiva. Tal es el caso, que se los detalla como los actos antijurídicos que según la ley Penal vigente (o socialmente reprochables, por lo que se estima factible su penalización futura) son realizados con empleo de máquinas automáticas de procesamiento de datos[28].

[24] Ibidem. Pág. 2.
[25] Ibidem. Pág 3.
[26] JIJENA LEIVA, R. (2012). *La criminalidad informática: situación de lege data y lege ferenda en CHILE.* Informática y Derecho. Pág. 54.
[27] ACURIO DEL PINO, S. (2011): *Delitos informáticos: Generalidades*. Pág. 9. Consultado el 11 de Abril de 2023. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
[28] DONOSO ABARCA, L. REUSSER MONSÁLVEZ, C.(2021). Op. Cit. Pág. 101.

Tal es asimismo la opción que en su momento adoptó el catedrático Antonio E. Pérez-Luño, quien amplió el concepto no solo a las conductas incriminadas de *lege lata*, sino de propuestas de *lege ferenda*, o sea, a programas de política criminal y legislativa, sobre aquellos comportamientos todavía impunes que se estima merecen la consiguiente tipificación penal[29].

En el caso de la Unión Europea, no se distingue sustancialmente si el elemento informático que justifica el tipo especial de delito se encuentra en el objeto, o fin mismo del delito (como puede ser la intromisión en la red interna de un banco para obtener los antecedentes comerciales de un tercero), o si consta en el mero medio para la realización de un fin ilícito (como puede ser la estafa vía Internet). Para ella, los dos casos anteriores son considerados como delitos cibernéticos o informáticos[30].

Si bien se puede establecer consenso de la sinonimia entre delitos cibernéticos e informáticos por parte de la doctrina, la Organización de Naciones Unidas se aparta de esta consideración y propone la noción de delitos cibernéticos en dos dimensiones distintas: la primera de ellas es definida como delito cibernético en sentido estricto o "delito informático";[31] la segunda la define como delito cibernético en sentido lato o "delito relacionado con computadoras"[32]. Para efectos de esta memoria, y comprender de la mejor forma posible, al fondo que se quiere llegar, se entenderá como sinónimos, el delito informático, con el ciberdelito, que se encontrarán participativos en gran parte de este trabajo, porque son términos fundamentales.

Abordando el delito informático desde una perspectiva acorde con la Teoría del Delito, se configura de la siguiente forma[33]:

a. La conducta humana: se expresa en el tipo delictivo a través del verbo rector, puede convertirse en una acción positiva (acción), o por el contrario, en una omisión. En el caso de los delitos informáticos, se comete un delito cuando el sujeto activo del delito o autor del mismo destruye, inutiliza, hace mal uso, revela, difunde, modifica, altera,

[29] PÉREZ-LUÑO, A.(1996). *Manual de informática y derecho*. Editorial Ariel. Barcelona. Pág 205-218.
[30] Lara, J. C., MARTÍNEZ, M., & VIOLLIER, P. (2014). *Hacia una regulación de los delitos informáticos basada en la evidencia.* Revista Chilena De Derecho Y Tecnología, 3(1). Pág 105. Disponible en: https://doi.org/10.5354/0719-2584.2014.32222.
[31] Ibidem.
[32] Ibidem.
[33] Cfr. ESPINOZA CORREA, C. (2014). *Delitos Informáticos y la Ley 19.223.* Revista Actualidad Jurídi-ca. 29: 554-555.

suprime, desestabiliza, interfiere o explota la información contenida en un **sistema de tratamiento automatizado de la misma o al mismo sistema en sí,** sin el consentimiento de la persona física o jurídica afectada.

b. El sujeto activo: se refiere a la persona que comete el delito. En términos generales, no hay requisitos especiales en relación con el sujeto activo. De esta forma, cualquier persona puede ser autora de este delito, independientemente de sus circunstancias.

c. El sujeto pasivo: se refiere a la persona natural o jurídica que resulta directamente afectada por el hecho delictivo como titular de los bienes jurídicos a proteger.

d. El objeto jurídico: es aquel bien jurídico que se pretende proteger. En el caso de los delitos telemáticos, los bienes jurídicos habitualmente afectados son la intimidad o privacidad de los datos personales, el patrimonio, la honra, la fe pública, etc. Los derechos e intereses legítimos afectados dependerán de la naturaleza de la interceptación, modificación, supresión, etc., para comprobar qué derechos jurídicos se han vulnerado.

Autores como M. López y C. Magliona sostienen que los delitos informáticos son de naturaleza pluriofensiva o compleja, es decir, se caracterizan por amparar simultáneamente múltiples intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo[34].

e. Objeto "material": Se refiere a la cosa o persona en la que recae la conducta delictiva de un delito informático. Ya no hablamos y entendemos objetos materiales en un sentido concreto o literal, aquí estamos hablando más de objetos inmateriales, porque los objetos son intangibles, electrónicos, son datos y software de programas. No son bienes u objetos de propiedad física, sino simplemente pulsos electromagnéticos.

f. Medio de ejecución: Tales delitos se ejecutan con la ayuda de un soporte lógico, la computadora, la telemática o cualquier otro medio utilizando un sistema informático.

[34] MAYER LUX, L. & VERA, J. (2020). *La falsificación informática:. ¿Un delito necesario?.* Scielo. Consultado el 21 de Marzo de 2023. Recuperado de: https://www.scielo.cl/scielo.php?pid=S0719-25842022000100261&script=sci_arttext

Ahora bien, después de concentrarnos en la definición y marco de lo que comprendemos por delitos informáticos, es necesario de igual forma constatar algunas formas de comisión de este tipo de delito. Acurio del Pino realiza una clasificación, donde los delitos informáticos tienen la calidad de[35]:

1) Fraude: Se define como el delito de alterar o manipular los datos y programas de un sistema informático. El concepto de fraude informático a veces se relaciona con otros delitos informáticos u otras contrapartes del ciberdelito. Por ejemplo, el fraude informático está asociado con el hacking, un concepto que se utiliza de forma imprecisa y casi como sinónimo de ciberdelincuencia. Ahora bien, en la taxonomía en torno al fraude se encuentran:

a) Datos Falsos o Engañosos (Data diddling): Es la manipulación de datos informáticos para crear u obtener pasos falsos en transacciones corporativas. Ocurre cuando se introducen incorrectos o se han manipulado datos del sistema lógico. Se considera que el caso más común de este tipo es la creación o manipulación de entradas informáticas para producir falsos movimientos, alteraciones, modificaciones o alteraciones de una transacción corporativa.

b) Manipulación de Programas o los Caballos de Troya (Trojan horses) : Este delito incluye la modificación de programas existentes en un sistema informático o la inserción de nuevos programas o nuevas subrutinas. Una forma de manipulación de programas es la inserción secreta de instrucciones de computadora en un programa de computadora para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c) Técnica del Salami (Rounching down): implica colocar instrucciones en un programa para transferir dinero de múltiples cuentas corrientes a una cuenta específica. En este modus operandi es que el criminal lo que hace es sacar o retirar datos o información reiteradamente en transacciones financieras de una cuenta determinada, de manera que el programa manda la instrucción de remitir dinero de esa cuenta a otras cuentas corrientes.

[35] Cfr. ACURIO DEL PINO, S. Santiago (2011). Op. Cit. Pág. 23-29.

d) Falsificaciones informáticas: Como objeto: Cuando se alteran los datos de los documentos almacenados en soporte informático. Como instrumentos: las computadoras también se pueden usar para falsificar documentos con fines comerciales.

Ocurre cuando los datos ya almacenados en el sistema de procesamiento de información cambian automáticamente. Esta forma de comisión ocurre, a modo de ejemplo, cuando una fotocopiadora de alta definición recrea un documento original y luego lo modifica para crear documentos falsificados sin tener que recurrir al original.

e) Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. Este modo delictivo consiste en codificar información electrónica falsificada. Suele referirse, a modo de ejemplo, en la falsificación de instrucciones que se le hacen a los cajeros automáticos.

f) Phishing: Esta forma de delito tiene como objetivo robar la identidad al sujeto pasivo, y se logra mediante la recopilación de datos como números de tarjetas de crédito, contraseñas, información personal y datos personales en general. Su accionar se efectúa mediante engaños que se realizan generalmente a través de un correo electrónico o ventana emergente. También existe una nueva modalidad de Phishing que es el llamado Phishing Segmentado o Spear Phishing, el cual ataca a grupos determinados, es decir, se busca grupos de personas vulnerables a diferencia de la modalidad anterior[36].

El phishing implica una obtención fraudulenta de datos de identidad personales de clientes de bancos y de sus cuentas bancarias o tarjetas de crédito[37], orientada a ejecutar transacciones electrónicas a favor del agente o de terceros.

2) Sabotaje informático: radica en la acción de borrar, suprimir o modificar sin autorización los datos de un sistema lógico informático con la intención de interferir con su operación normal. Se puede enviar a través de los siguientes métodos:

[36] Ibidem.
[37] MAYER LUX, L., & OLIVER CALVERÓN, G. (2020). *El delito de fraude informático: concepto y deli-mitación*. Revista Chilena De Derecho Y Tecnología, *9*(1). Pág. 151-184. Recuperado de: https://doi.org/10.5354/0719-2584.2020.57149.

a) Virus informáticos y malware: Los virus informáticos son elementos informáticos que se replican y propagan dentro de los sistemas informáticos a los que acceden. El malware utiliza la misma técnica, desactiva la administración de la computadora de una computadora y comienza a propagar código malicioso.

b) Gusanos: Es la infiltración en programas de tratamiento de datos con la finalidad de alterar o destruir datos legítimos. Se diferencia de un virus en que no puede reproducirse, pero los efectos de un ataque de gusano pueden ser tan graves como los de un ataque de virus.

c) Bombas Lógicas (Logic bombs): Corresponde a la programación de la modificación o destrucción de datos en un momento del futuro.

d) Ciberterrorismo: Es un acto telemático que tiene como objetivo desestabilizar un país o presionar a un gobierno en particular utilizando métodos que entran en la categoría de delitos informáticos.

e) Ataques de denegación de servicio: se basan en la utilización máxima de los recursos lógicos del sistema para que nadie más pueda utilizar el sistema. Se perjudica notablemente, de esa forma, la actuación del sistema, especialmente si debe dar servicio a una multiplicidad de usuarios.

3) Espionaje informático: Corresponde a la obtención de manera ilícita, dolosa y sin autorización de datos o información relevante y programas o software de computadora.

a) Data leakage: o de otra manera llamada "fuga de datos", implica la divulgación no autorizada de los datos sensibles y reservados en poder de una empresa realizada por parte de un hacker (pirata informático). Desde la doctrina, hay autores que se refieren con respecto a este tema expresando que *"la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"*[38].

[38] ACURIO DEL PINO, S. (2011). Op Cit. Pág 27.

b) Copia ilegal o hurto de programas o software: se refiere a un delito tipificado y sancionado en la ley 17.336 de Propiedad Intelectual. El autor Acurio del Pino, expresa *"que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar, el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática"*[39].

4) Acceso no autorizado a servicios informáticos:

a) Superzapping: Concierne a un programa que tiene por objeto cambiar, copiar, utilizar o borrar archivos informáticos, aunque estén protegidos. Se conoce también con el nombre de llave maestra.

b) Trap doors: Consiste en implementar interrupciones en la lógica del programa para ir comprobando, en un proceso complejo, las operaciones o resultados intermedios y producir salidas de control o guardar esta codificación. También se conocen con el nombre de puertas falsas.

c) Wiretapping: Se refiere a la interferencia de las líneas telefónicas de transmisión de datos para obtener la información que se transmite a través de ellas. Esto se puede hacer usando una radio, un módem o una impresora.

d) Hackers (sentido genérico): Personas que aprovechan las imperfecciones en las medidas de seguridad de las páginas web o plataformas digitales para obtener acceso a las mismas. Se puede verificar que son actores que realizan tales intrusiones desde una ubicación fuera del entorno telemático comprometido de la persona natural o jurídica afectada.

[39] Ibidem. Pág 28.

5) Piggybacking and impersonation: dentro de esta forma de operar hay un concurso de delitos en donde se encuentran: el delito de suplantación de identidad y el delito de espionaje informático. Este tipo de actividad se caracteriza en que los delincuentes utilizan la identidad de otra persona para cometer otro delito informático.

Con todo lo señalado, cabe destacar que los delitos informáticos no poseen una definición exclusiva estándar. Sin embargo, nuestra legislación sanciona actualmente al que destruya, acceda o inutilice un sistema de tratamiento de información[40]. Así mismo, protege los datos contenidos en él, de forma que se establecen sanciones a través de penas para quienes se apoderen, intercepten, difundan o destruyan la información allí contenida.

Desde el punto de vista de la ilicitud, el conjunto de delitos informáticos en sentido estricto, esto es, de los comportamientos que afectan el software o soporte lógico de un sistema de tratamiento automatizado de la información[41], está compuesto entonces por tres ilícitos principales: el sabotaje informático, el espionaje informático y el fraude informático[42]. En el momento en que estos actos ilícitos tienen por fin destruir, eliminar o inutilizar el sistema de tratamiento automatizado de datos o la información contenida en sí, es cuando hablamos de delitos digitales de "cracking"[43]. En suma, los delitos informáticos son **nuevas formas de cometer fraude o estafa** en un sentido amplio, esto es, dentro de la esfera de los delitos telemáticos.

Por último, antes de concluir este capítulo es necesario exponer, para obtener una mejor comprensión de los delitos informáticos, que ellos no se encasillan en una noción tradicional de fraude. En este contexto, el ciberdelito no se limita al ánimo de lucro, que tiene un sentido monetario, o a la afectación del patrimonio de una persona, va un paso más allá. Hay una amplia variedad de bienes jurídicos que pueden ser afectados, no solamente por ejemplo el patrimonio de una persona, sino que de igual modo, puede afectar la honra, privacidad de sus datos personales, etc. No hay duda de que, no es posible aplicar el delito de fraude tradicional de inmediato, porque no hay engaño directo involucrado induciendo a una

[40] Ley 21.459. Artículo 1.
[41] MAYER LUX, L., & OLIVER CALDERÓN, G. (2020). Op Cit. 151-184.
[42] MAYER LUX, L. (2018). *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos.* Año N°24 . N°1. Ius et Praxis. Pág. 161. Recuperado de: https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf.
[43] HERNÁNDEZ, C. (1999). *Hackers, Los Piratas del Chip y de Internet.* Libro electrónico gratuito. Pág. 34. Disponible en: http://.perso.wanadoo.es/snickers.

persona a error. Aquí lo que pasa, es que se engaña al sistema lógico de tratamiento de datos, de tal forma que no por eso vamos a entender que objeto material del delito informático es como el hardware físico o la computadora misma, sino que, el objeto material, elocuentemente es el soporte lógico o sistema informático del afectado ocasionando vulnerabilidades en su sistema.

III.2 Fraude Informático

Dentro de los delitos informáticos, el fraude informático continúa siendo el centro de estos, por su impacto económico y la frecuencia práctica que simboliza su ejecución[44]. El fraude informático se puede caracterizar, a modo genérico, como un delito que comete el que manipula un sistema informático, mediante la **introducción, alteración, daño o supresión de datos informáticos o lo hace a través de cualquier interferencia en el funcionamiento de un sistema informático**[45]**.** Se necesita que la **acción cause un perjuicio a otro, además de que aquella persona que la ejecute lo haga para obtener un beneficio económico para ella o para un tercero.**

Autor en este contexto, también se le considerará al que facilita los medios para cometer el delito, conociendo o no pudiendo menos que conocer que la conducta es delictiva.

Las penas para el fraude informático son[46]:

- Si el valor del perjuicio supera las 40 unidades tributarias mensuales (UTM): presidio menor en sus grados medio a máximo (541 días a 5 años) y multa de 11 a 15 unidades tributarias mensuales.
- Si el valor del perjuicio supera las cuatro UTM y no superara las 40 UTM: presidio menor en su grado medio (541 días a 3 años) y multa de 6 a 10 UTM.
- Si el perjuicio no supera las 4 UTM: presidio menor en su grado mínimo (61 días a 540 días) y multa de 5 a 10 UTM.
- Pero si el valor del perjuicio supera las 400 UTM, la pena será de presidio menor en su grado máximo (3 años y 1 día a 5 años) y multa de 21 a 30 UTM.

[44] MAYER LUX, L., & OLIVER CALDERÓN, G. (2020). Op Cit. 151-184.
[45] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. (2022). *Delitos Informáticos.* Consultado el 29 de Febrero de 2023. Recuperado de: https://www.bcn.cl/portal/leyfacil/recurso/delitos-informaticos.
[46] Ibidem.

Abordando los problemas de delimitación del fraude informático, se pueden sistematizar de la siguiente manera:

En primer lugar, la noción de fraude informático a veces es vinculada con conductas que en realidad corresponden a etapas de ejecución imperfecta (delito tentado o frustrado) e incluso a actos preparatorios de un fraude propiamente tal. En especial, los comportamientos de phishing y pharming, que se ejecutan en el contexto de operaciones bancarias por lo general, son un buen ejemplo del relajo con la que se emplea en reiteradas ocasiones aquella expresión. Apreciándose de otro modo, aunque esas conductas en rigor no se identifican con la provocación de un perjuicio patrimonial a través de la manipulación o alteración de datos de sistemas informáticos, por lo general se incluyen dentro de una noción amplia de fraude informático[47].

Por otra parte, el concepto de fraude informático en ocasiones suele **vincularse al fraude informático con el hacking**, sinónimo casi de ciberdelito[48]. De cualquier forma, si la palabra hacking se entiende como el acceso indebido a datos o programas de sistemas informáticos, podrá advertirse que para cometer fraude informático se hará vital acceder de forma indebida a los datos o programas en cuestión. He aquí el problema, puesto que conlleva a que ambas conductas se encuentren en una potencial relación concursal[49].

Al mismo tiempo, puede plantearse una relación entre conceptos, **fraude informático** y **sabotaje informático**. El primero se asocia con la **alteración de datos,** mientras que el segundo con su **destrucción**. Tal relación se constata si se revisa la descripción que el *"Convenio sobre Ciberdelincuencia del Consejo de Europa"* (CCCE) prevé para lo que denomina "ataques a la integridad de los datos"[50] y "fraude informático"[51], las cuales comparten conductas, a modo de ejemplo, por relevancia se encuentran aquellas que alteran o suprimen datos.

En otro orden de ideas, el delito de fraude informático tradicionalmente ha sido relacionado con el delito de estafa, al punto que en legislaciones como española se le regula

[47] MAYER LUX, L., & OLIVER CALDERÓN, G. (2020). Op Cit. 151-184.
[48] Ibidem.
[49] Ibidem.
[50] CONVENIO SOBRE LA CIBERDELINCUENCIA. Artículo 4, número 1.
[51] Ibidem. Artículo 8.

sucesiva o conjuntamente, lo que ha contribuido a aclarar las diferencias entre ambos ilícitos, por lo que importante es ver legislación comparada al respecto y el tratamiento que se le da en otros países al fraude informático. En ese mismo sentido, si bien ambas figuras delictivas tienen varios elementos en común, partiendo por la exigencia de un perjuicio patrimonial ajeno, **el punto que las distingue es el medio necesario para provocarlo, el cual, por una parte es la manipulación de datos y, por la otra, el medio es el engaño[52].**

III.3 Legislación comparada (España) en torno al fraude informático

El fraude informático o estafa por medios informáticos es aquella tipología del cibercrimen en el que se da la defraudación por medios informáticos, en otras palabras, la utilización del sistema informático como medio para transferir los activos patrimoniales a favor del autor y el desplazamiento es siempre virtual, inaprensible[53]. Las denominaciones han sido diversas: estafa telemática, estafa por computación, fraude informático. El fraude informático se regula en el art. 248.2[54] del Código Penal Español de 1995, siendo considerado por el legislador como una modalidad de la estafa, aplicándosele los preceptos relativos a la penalidad de la estafa y agravaciones, si bien las afinidades que presenta con la estafa genérica del art. 248.1º son mínimas[55].

Se instaura por el legislador al comienzo del artículo 248.2 *"también se consideran reos de estafa"*, expresión que a juicio de la doctrina cierra cualquier polémica y ello conlleva tres cosas: **el sujeto activo menoscaba el patrimonio ajeno, la conducta fraudulenta consiste en manipulación informática o artificio semejante y la posibilidad de aplicar la pena de estafa y agravaciones al tipo del art. 248.2[56].**

---

[52] MAYER LUX, L., & OLIVER CALVERÓN, G. (2020). Op. Cit.
[53] ÁLVAREZ, M. (2001) *Consideraciones político criminales sobre la delincuencia informática.* Dialnet. Pág 274. Consultado el 10 de Septiembre de 2022. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=289088.
[54] Código Penal español. Art. 248.2: "2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".
[55] García, J. (2008) *El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico***.** Pág. 293. Disponible en: https://revistas.comillas.edu/index.php/revistaicade/article/download/357/283.
[56] CÓRDOBA, J y GARCÍA, M. (2004) *Comentarios al Código Penal*, *parte especial*. Tomo I. Aranzadi. Madrid-Barcelona. Pág 770.

Concretamente, el delito de estafa en un delito de relación, sin embargo, si la conducta se realiza frente a una máquina mediante las formas establecidas en el artículo 248.2, entonces estamos frente a la estafa informática[57].

En resumen, el fraude informático tiene como elemento común el ánimo de lucro con la estafa genérica, no tiene los elementos del error y el engaño como la estafa, no obstante, se diferencia en otros, como por ejemplo, la concurrencia de la manipulación informática o artificio semejante y la transferencia no consentida de activos patrimoniales en perjuicio de tercero[58]. Dicho esto se deduce que **el bien jurídico protegido es el patrimonio.**

Ahora bien, el sujeto activo puede ser cualquier persona, por un lado, las legitimadas para acceder al sistema, como también terceros no autorizados, siempre que utilicen manipulación informática o treta semejante. El sujeto pasivo es aquel titular del patrimonio, que puede ser perjudicado desde el punto de vista de la responsabilidad civil.

Cabe mencionar que la criminalidad informática afecta de múltiples formas en el ámbito criminal: modifica las formas criminales tradicionales (entre ellos estafa y fraude), nacen nuevos crímenes y se altera su percepción[59]. Se hace desafiante a su persecución, saber que, históricamente, la criminalidad informática tiene como primera forma de manifestación al fraude informático[60].

IV. Capítulo 2. LA CIBERSEGURIDAD EN CHILE

IV. 1 Realidad actual en Chile de la ciberseguridad

En atención a la naturaleza global del ciberespacio y su amplio campo, los riesgos provienen de amenazas provenientes tanto de Chile como igualmente del exterior, y poseen diversos orígenes, entre los que destacan en especial para nuestro país[61]:

[57] RODRÍGUEZ, L.(coord.) y otros.(2005). *Código Penal*. Madrid: La Ley. Pág. 549.
[58] GARCÍA, J. (2008). Op. Cit.
[59] PICOTTI, L. (1989). *"La criminalità..."*, cit., Pág. 31.
[60] GARCÍA, J. (2008) Op. Cit. Pág. 303.
[61] MINISTERIO DE INTERIOR Y SEGURIDAD PÚBLICA (2017). *Política Nacional de Ciberseguridad.* Pág. 36. Disponible en: https://digital.gob.cl/biblioteca/estrategias/politica-nacional-de-ciberseguridad-2017-2022/.

a) **Incidentes internos:** fugas involuntarias de información, interrupción accidental de sistemas informáticos, u otros incidentes involuntarios que pueden afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

b) **Desastres naturales o fuerza mayor:** terremotos, inundaciones u otros desastres que puedan afectar al ciberespacio, debido a la destrucción de infraestructuras físicas esenciales para la disponibilidad de la información.

c) **Actividades de espionaje y vigilancia llevadas a cabo por actores estatales:** conductas que afectan la confidencialidad de la información, mediante su sustracción con fines políticos o estratégicos. En particular, destacan acciones utilizando herramientas sofisticadas conocidas como APT (en español, Amenazas Avanzadas Persistentes), que a su vez pueden valerse de vulnerabilidades informáticas no publicadas de las tecnologías en uso.

d) **Ataques de denegación de servicio y denegación distribuida de servicios (DOS y DDOS):** En páginas anteriores ya se ha hablado respecto a este tipo de ataque, pero poniéndolo en contexto con relación al capítulo presente, consisten en la sobrecarga intencional de servicios que se proveen en un sistema informático, que puede ser conducida desde un punto de la red o distribuirse para coordinar el ataque desde varios puntos, muchas veces mediante dispositivos infectados con programas maliciosos, con el fin de cumplir dicho propósito[62].

e) **Cibercrimen:** actividades criminales cometidas contra componentes del ciberespacio (acceso no autorizado, sabotaje de información, robo de información, secuestro de esta o ransomware, como también empleando herramientas del ciberespacio como medio de comisión, phishing, pharming, fraudes virtuales, y otros).

f) **Ataques a infraestructuras críticas mediante el ciberespacio:** esto mediante la alteración en el funcionamiento de infraestructuras críticas (físicas o de la información) realizada por medios electrónicos. Por ejemplo: disrupción masiva de

[62] MICROSOFT. *Definición de los ataques DDOS.* Consultado el 12 de Marzo de 2023. Recuperado de: https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-ddos-attack.

sistemas financieros, intervención de servicios básicos, daños físicos a infraestructuras, y otros relacionados.

Todos estos riesgos y amenazas afectan la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información en el ciberespacio, y en el mediano plazo, sin lugar a dudas puede afectar sustantivamente al desarrollo del país en el entorno del ciberespacio. Lo mencionado nos priva de los beneficios asociados al gobierno digital, comercio electrónico, formas de organización social facilitadas por el ciberespacio, y amenazando la seguridad de las personas e instituciones en este ambiente. Algunos casos aquí presentados pueden caer en más de una categoría.

Tomando como referencia el nivel de la región[63], los países que han registrado el mayor número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Accesos o robo de información desde un ordenador infectado (denominados botnets) predominaron en la región. Incluso, un tipo específico de este código malicioso llamado "Dorkbot" generó más de 80 mil acciones contra el sistema virtual, concentrándose en Chile (44%), Perú (15%) y Argentina (11%)[64].

En Chile, dentro del ámbito público de infraestructura crítica, la Red de Conectividad del Estado (RCE) sufre numerosas actividades maliciosas o sospechosas. Existen registros de incidentes vinculados a ataques de denegación distribuida de servicios (DDoS) o alteraciones de sitios webs gubernamentales, observándose un importante crecimiento en esta materia, desde el año 2010[65].

Ahora bien, en el último tiempo, nuestro país viene manifestando un alza sustantiva en ciberataques. En el año 2022 organismos como el Poder Judicial (PJUD), el Estado Mayor Conjunto (EMCO), el Servicio Nacional del Consumidor (SERNAC) y la Comisión Nacional de Acreditación (CNA) han sido algunos de los afectados.

[63] PRANDINI, P. MAGGIORE, M. (2013). *Ciberdelito en América Latina y el Caribe. Una visión desde la sociedad civil.* Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe. Pág. 3.
[64] EQUIPO CEEAG. (2016). *Desafío para afrontar la ciberguerra.* Tema De Investigación Central De La Academia. Pág. 147 - 164. Disponible en: https://publicacionesacague.cl/index.php/tica/article/view/180.
[65] MINISTERIO DE INTERIOR Y SEGURIDAD PÚBLICA (2017). Op. Cit. Pág. 37.

Los **ataques van desde la retención de datos a cambio de cobros hasta filtraciones de correos y otras informaciones**. Algunas de estas vulneraciones, han dejado en claro la falta de preparación de estos organismos, como asimismo se deja expuesto que falta invertir más en esta materia, para poder tener policías con suficiente capacidad técnica, como asimismo un Ministerio Público capaz, para poder investigar y combatir casos complejos en relación al delito informático.

Profundizando más en este tema, dos casos mediáticos ocurridos en Chile durante el año 2022 relacionados con un ataque cibernético, fue por una parte el ataque en contra del Poder Judicial[66], como por otro lado, el ocasionado en contra del Estado Mayor Conjunto de Chile[67].

A modo de ejemplo, mencionado lo dicho con anterioridad, en relación con el caso del Poder Judicial chileno. Con fecha 25 de Septiembre de 2022 se dedujo un ataque cibernético en contra de computadores pertenecientes al Poder Judicial. Tras ser víctima de un malware, se conoció que gran parte de sus equipos operan con sistemas casi obsoletos y poco actualizados, como Windows 7, por ejemplo. La Corporación Administrativa del Poder Judicial informó que en septiembre la institución fue afectada por un incidente de ciberseguridad, provocado por una campaña masiva “ransomware”. A propósito de esa infección se procedió entonces primero a detectar 150 computadores comprometidos con una infección de virus informático y otros tantos se fueron detectando con posterioridad, los cuales fueron desconectados. Se estima que no hubo posteriores infecciones, sino que hubo una extensión a computadores que luego se revisaron[68].

Asimismo, en el año 2022, específicamente durante el primer semestre ocurrió un hackeo mediático, masivo al Estado Mayor Conjunto, en donde se expuso miles de documentos relacionados con áreas sensibles de la defensa. En resumen, más de 400 mil mensajes de correos electrónicos del Estado Mayor Conjunto que fueron expuestos incluyen

---

[66] GONZÁLEZ, C. (2022). *Alerta por ataque informático al Poder Judicial: Jueces deben realizar audiencias desde celulares y no abrir correos dudosos.* Diario El Mercurio On-Line. Consultado el 28 de Ocubre de 2022. Recuperado de: https://www.emol.com/noticias/Nacional/2022/09/26/1073829/ataque-informatico-al-poder-judicial.html.

[67] SEPÚLVEDA, N. (2022*). Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa.* CIPER. Recuperado de: https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/.

[68] PODER JUDICIAL REPÚBLICA DE CHILE. (2022). *Poder Judicial presenta denuncia criminal por incidente de ciberseguridad.* Consultado el 10 de Diciembre de 2022*.* Recuperado de: https://www.pjud.cl/prensa-y-comunicaciones/noticias-del-poder-judicial/79577.

documentos rotulados como “reservado”, “secreto” y “ultrasecreto”, de áreas sensibles de la defensa, como la estrategia de ciberseguridad, el sistema de monitoreo de comunicaciones satelitales en las fronteras y programas para almacenar bases de datos de inteligencia. La filtración incluye informes del Comando Conjunto Norte y el Comando Conjunto Austral, además de datos de los agregados de defensa en todo el mundo[69].

Según los datos proporcionados por la agencia gubernamental chilena que lleva el nombre de Equipo de Respuesta ante Incidentes de Seguridad Informática (en adelante CSIRT), en lo que va del año 2022 se emitieron múltiples informes de vulnerabilidad similares a los que dieron pie a los incidentes registrados en el Poder Judicial y del Estado Mayor Conjunto. El grueso de las alertas de la CSIRT en relación con entidades públicas se refiere a vulnerabilidades que afectan a páginas web[70].

Acorde a los datos compartidos por el gobierno de Chile, el subsecretario del Interior, Manuel Monsalve, en sesión especial desarrollada en el Senado el jueves 29 de Septiembre de 2022 con motivo de la inauguración del mes de la ciberseguridad, reconoció que mensualmente Carabineros recibe 14,4 millones de ataques cibernéticos. De esta manera se concluye que en Chile, desde una perspectiva de su estado actual, falta de una manera urgente alcanzar mejores estándares en torno a la ciberseguridad. Algunos de los desafíos más importantes es mejorar la capacidad del Estado y de los privados en la identificación y gestión de riesgos que significa la digitalización de nuestra vida cotidiana[71].

Es imprescindible que la legislación chilena esté en constante avance en torno a la ciberseguridad, pero en conjunto con aquello, es necesario ampliar la tipificación de los nuevos delitos constantemente emergentes, en un mundo cibernético con mayor creatividad a la hora de crear un nuevo virus o malware para afectar a la comunidad. Sumado a lo antedicho, se hace fundamental el adiestramiento y perfeccionamiento técnico de las policías encargadas y especializadas en combatir estos tipos de delitos, dado que, será de nula eficacia, si las policías no poseen ni las facultades, ni las herramientas pertinentes que se necesitan durante la investigación y persecución de delitos informáticos.

[69] SEPÚLVEDA, N. (2022). Op. Cit.
[70] BATARSE, C. (2022). *Gobierno registra 170 alertas por vulnerabilidad similares a los hackeos del Poder Judicial y las Fuerzas Armadas.* Diario La Tercera. Consultado el 10 de Diciembre de 2022. Recuperado de: armadas/TYYG46Q6KFD4LDC7IJPU63TQOE/.
[71] Ibidem.

Algo a remarcar en torno al combate del delito informático, como expertos en el tema lo han indicado, entre ellos, el director de Nivel 4 Cybersecurity Fernando Lagos, expresó a través de su cuenta de Twitter, es una forma de enfrentar este tipo de delitos, inclinado hacia una prevención del delito por sobre un ataque de este, posterior a la comisión del mismo, en donde textualmente expresa que *"Cuando falla la prevención de un incidente o de un ciberataque, no puede fallar la forma de gestionar dicho incidente, incluyendo el cómo se comunica de forma interna y externa…"*[72]. Este punto llama considerablemente la atención debido a que no está lejano a lo que postula, por ejemplo, la Oficina de Naciones Unidas contra la Droga y el Delito, la cual relata dentro de los tipos de investigación, la forma proactiva ha sido una iniciativa desarrollada con mayor fuerza en los últimos años por sobre las reactivas[73].

En suma, la vigilancia proactiva se centra contra amenazas graves o nuevas de delitos en aumento para reducir el daño que pueden causar, en lugar de garantizar respuesta al delito una vez que ha sido cometido y denunciado posteriormente. Las metodologías del investigador siguen siendo las mismas, sin embargo, los delitos a los que se aplican, se detectan mediante la investigación. A modo de ejemplo, se pone a una figura delictiva prominente en el centro de un análisis completo, después del cual se le someterá a una serie de acciones hasta eliminar la amenaza que representa porque ha sido enjuiciado o se han eliminado los medios por los cuales se iba a cometer el delito.

IV.2 Ley Marco de Ciberseguridad

Si se piensa en la ley de delito informático, como su nombre lo indica, en simples palabras, está orientada a sancionar conductas que son reprochables totalmente para la sociedad. Ahora bien, lo que vendría una nueva ley marco **es organizar conductas y entregar**

[72] LAGOS, F. (2022). (Comentario en la página Web). Twitter. Consultado el 2 de Noviembre de 2022. Recuperado de:https://twitter.com/Zerial/status/1574401080385048577?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1574401080385048577%7Ctwgr%5Ee3f4fa541f46859110767a749411011f44879c5e%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.biobiochile.cl%2Fnoticias%2Fciencia-y-tecnologia%2Fpc-e-internet%2F2022%2F09%2F30%2Fciberataques-a-entidades-gubernamentales-por-que-ocurren-y-que-se-puede-hacer-para-evitarlos.shtml.

[73] UNODC. (2010). *Informe Mundial de UNODC sobre trata de personas: las crisis cambian los patrones de la trata de personas y dificultan la identificación de las víctimas.* Oficina de las Naciones Unidas contra la Droga y el Delito en México. Recuperado de: https://www.unodc.org/lpomex/es/noticias/enero-2023/informe-mundial-de-unodc-sobre-trata-de-personas_-las-crisis-cambian-los-patrones-de-la-trata-de-personas-y-dificultan-la-identificacin-de-las-vctimas.html.

ciertos estándares a todos quienes van a participar en equipos de la infraestructura tecnológica[74].

Sin ley expresa, se dialoga a modo de ejemplo de la obligación de ciberseguridad de un distribuidor de energía. Hay una variedad de operadores que no todos tienen el mismo nivel de complejidad y, sin embargo, las obligaciones podrían o las cargas podrían ser las mismas para todos. Si se tiene, por ejemplo, un operador que estaba abasteciendo de energía al Gran Santiago versus a un operador fotovoltaico que está en Rengo, obviamente el impacto y las consecuencias de la afectación de ambas infraestructuras es diferente. Entonces, lo que puede realizar la ley Marco de Ciberseguridad es establecer estándares en torno a la proporcionalidad para los distintos roles y para distinta envergadura de los operadores de infraestructura crítica.

IV.3 Política nacional de ciberseguridad en Chile

El estado de Chile ha adoptado políticas de estado en torno a la ciberseguridad para dar mayor seguridad tanto a las instituciones del Estado como a la población chilena en su conjunto. Dentro del marco de las políticas públicas encontramos que para el año 2022 se hacía el compromiso que[75]:

a) El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.

b) El Estado velará por los derechos de las personas en el ciberespacio.

c) Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.

[74] PROYECTO DE LEY 14.847-06. (2022). *Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.* Ingreso de Proyecto. Pág. 6. Consultado el 30 de Abril de 2023. Disponible en; https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06.
[75] BARRIOS, V. (2018). *Política Nacional de Ciberseguridad: 2017-2022*. Pág. 3-4. Biblioteca del Congreso Nacional de Chile. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf .

d) El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.

e) El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos.

Relacionado a política nacional de ciberdefensa el gobierno chileno ha tomado cartas en este asunto, por lo cual el Ministerio de Defensa, durante el año 2017 dio un paso, se tomó mayor consideración a este tema y se propuso como objetivo preparar y publicar políticas específicas de ciberdefensa, que contemplen las definiciones políticas en torno a cómo serán protegidas estas redes, además de establecer cómo las capacidades de la Defensa Nacional pueden colaborar en la formación de un ciberespacio libre, abierto, seguro y resiliente para el país.[76]

Ahora bien, desde la perspectiva de la política internacional para el ciberespacio, uno de los objetivos de alto nivel detallado en la presente política nacional dice relación con la cooperación y relación internacional en torno a la ciberseguridad en el contexto global. Sin embargo, es vital que el país integre de igual forma los objetivos relacionados con el desarrollo, derechos humanos, la defensa, entre otros, para consolidarlos e integrarlos en la política exterior de Chile.

Para cumplir con esta ambiciosa política nacional de ciberseguridad y siguiendo el ejemplo de diversos países que han iniciado este proceso hace algunos años, resulta fundamental para Chile contar con un modelo de gobernanza de la ciberseguridad que se haga cargo de, al menos, desempeñar las funciones que se identifican como esenciales, y que no están siendo abordadas o se ejecutan de manera descoordinada en el país.

Destacable es que en la política nacional de ciberseguridad se evaluó la creación de un consejo consultivo asesor, de integración multisectorial. Las funciones que se identificaron como esenciales son la gestión de relaciones interinstitucionales, gestión de incidentes, funcionamiento como punto de contacto nacional e internacional en este ámbito, función

[76] HORZELLA, B. (2021). *Política nacional de Ciberdefensa.* Biblioteca del Congreso Nacional de Chile. Pág. 3. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe_BCN__Politica_Nacional_de_Ciberdefensa.pdf

comunicacional, función normativa técnica y asesora en normativa general, función de seguimiento y evaluación de medidas. Lo anterior dio fruto y en 2019 se produjo la creación de la CSIRT, que ha sido un considerable avance del estado chileno en torno a la seguridad de la infraestructura crítica del país. Esta institución tiene como objetivo coordinar y apoyar las respuestas ante eventos o incidentes.[77]

Las medidas propuestas por la Política Nacional de Ciberseguridad tienen en especial consideración que Chile ostenta una de las mayores tasas de penetración de internet en América Latina, con más de un 70% de su población conectada[78], lo que permite que cada vez más y más ciudadanos puedan interactuar en este ambiente digital, aprovechando sus ventajas como la mensajería instantánea, la extensión de las redes sociales y la variedad de páginas web con acceso al comercio electrónico.

Sin embargo, este incremento en el uso tiene sus contras, entre los cuales es posible mencionar que aumenta la dependencia y vulnerabilidad frente a las redes. Hoy, esto se manifiesta en incidentes y ataques informáticos cada vez más frecuentes. Mejorar el nivel de seguridad de la información nacional es imprescindible, mediante la lucha eficaz contra el delito cibernético y garantizar que las personas ejerzan sus derechos en el ciberespacio de conformidad con la ley.

En el proceso de diseño de la Política Nacional de Ciberseguridad, dentro de las mayores dificultades, encontramos la falta de estudios e información sobre el estado de la seguridad digital, tanto en el sector público como privado, por una parte, dado al bajo nivel de madurez que hay en este ámbito, como también por la resistencia de las organizaciones a dar a conocer sus debilidades. Por ello es importante realizar estudios, ya sean a nivel doctrinario o informes, que permitan identificar los efectos que los diversos aspectos de la ciberseguridad pueden ir provocando a las ciencias jurídicas y el derecho, ya sea a nivel nacional como internacional[79].

[77] CSIRT. *Quiénes somos*. Consultado el 17 de Agosto de 2022. Recuperado de: https://www.csirt.gob.cl/quienes-somos/.
[78] ÁLVAREZ, D. (2017). *Los desafíos de la ciberseguridad en Chile.* Revista chilena de Derecho y Tec-nología. Consultado el 1 de Octubre de 2022. Recuperado de: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842017000200001.
[79] Ibidem.

Con lo expuesto, es necesario avanzar en una ley marco de ciberseguridad efectiva para el porvenir del país, además de establecer una ley de protección de datos personales y una agencia de ciberseguridad que pueda articular los esfuerzos de la CSIRT. De igual forma, es preciso contar con instituciones públicas y privadas, para prevenir, proteger, detectar, contrarrestar y responder a ciberataques sobre la infraestructura crítica del país. Una agencia que tenga facultades tanto sobre el sector público como el sector privado, con facultades normativas, de fiscalización y formación.

No obstante, nada de lo mencionado dará resultado, si la sociedad en su conjunto no considera la ciberseguridad del país a un nivel mucho más importante de cómo la aprecia al día de hoy. La colaboración entre los sectores público, privado y académico, es urgente, vital para crear las capacidades técnicas y humanas que tanto se necesitan para hacer frente a las dificultades de la ciberseguridad.

IV.4 Modelo de Madurez de capacidades de ciberseguridad para Naciones

A nivel mundial, el *Global Cyber Security Capacity Centre* de la Universidad de Oxford (en adelante Centro Global de Capacidad en Seguridad Cibernética), se encarga de realizar una medición y evaluación de seguridad cibernética de todos los países. Poniendo a disposición esta información para que los países puedan mejorar sus respectivas políticas internas en relación a la ciberseguridad.

Ofrecen justamente una perspectiva longitudinal a lo largo del tiempo de todos los países que se someten a esta evaluación y hacen un desarrollo detallado de la capacidad de seguridad cibernética de toda la región.

El objetivo del Centro Mundial de Capacidad en Seguridad Cibernética es aumentar la magnitud y efectividad del desarrollo de la capacidad en ciberseguridad, tanto en el Reino Unido como en el resto de países, a través de la implementación del Modelo nacional del estado de desarrollo de capacidad en materia de ciberseguridad. El Centro Mundial de Capacidad en Ciberseguridad espera ayudar a promover un ciberespacio innovador que respalde el bienestar, al ayudar a comprender la capacidad de ciberseguridad nacional, los derechos humanos y la prosperidad para todos los usuarios.

Para poder fundamentar sus observaciones detalladamente, el centro toma en consideración que la capacidad en ciberseguridad comprende cinco dimensiones[80]:

1. Formular políticas y estrategias en ciberseguridad;
2. Fomentar dentro de la sociedad una cultura responsable en ciberseguridad;
3. Desarrollar conocimiento en ciberseguridad;
4. Crear marcos regulatorios y legales efectivos; y
5. Controlar los riesgos a través de normas, organizaciones y tecnologías.

En ese sentido, Chile con los avances en ciberseguridad y creación de organismos encargados de la infraestructura crítica, asimismo con el progreso legal y políticas públicas en torno a este tema, se puede sostener que tiene un nivel de madurez "intermedio" en comparación con otros países de la región. Desde esa perspectiva se puede decir que Chile no está tan mal posicionado en esta materia. Ahora bien, hay muchos esfuerzos de la comunidad internacional orientados, a contribuir a que los países consigan subir sus estándares de ciberseguridad, siendo medios para lograrlo que: posean una ley de protección de datos, asimismo logren contar con una correcta prevención de delitos informáticos, que puedan gozar la implementación de una política nacional de ciberseguridad, la cual contribuya a formar, por ejemplo, un Equipo de Respuesta ante incidentes de Seguridad Informática a nivel conjunto de países.

Es trascendental que se apliquen medidas en los diversos países, dado que, a mayor seguridad en cada país, se obtendrá el efecto que se pueda brindar más seguridad a los países con los cuales se relacionan, dentro de un mundo donde la internet es fundamental para la interacción entre personas como de igual forma la economía, política, cultura, etc.

Actualmente, la primera política nacional ya está agotada y se está trabajando en la segunda política, de sumo interés a estudiar, porque la política de la inteligencia artificial tiene una serie de acciones a apreciar, entonces eso ha permitido que se haga una verificación de lo que fue realizado y en donde se avanzó, de esa manera poder visualizar si el país ha cumplido con las metas, pero sin dudas, a pesar de lo que se puede decir que aún falta mucho

[80] GLOBAL CYBER SECURITY CAPACITY CENTRE UNIVERSITY OF OXFORD. (2016). *Modelo de Madurez de Capacidades de Ciberseguridad para Naciones* (CNM). Pág 6. Disponible en: https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7840

camino, se ha avanzado considerablemente. Y esto viene de la mano con la pandemia que estalló a nivel mundial, como lo fue la del SARS-CoV 2, la cual, sin duda aceleró la importancia en general que los gobiernos le brindaron a sus políticas sobre este asunto, dado que la sociedad, cada vez con mayor fuerza, transita al mundo tecnológico virtual y de inteligencia artificial, para ejecutar variadas acciones de su vida cotidiana.

De todos modos, se hace urgente una tramitación más expedita y urgente de la ley marco sobre ciberseguridad e infraestructura crítica de la información, que desde el 15 de marzo de 2022 se mantiene en el Senado[81], y no solamente en la ley marco, sino que a futuro el legislador debe dar mayor auge en legislar, aprobar y contribuir a que la legislación nacional esté actualizada en torno a este tópico que en el futuro dará mucho que hablar, porque la sociedad se dirige cada vez más a un entorno conectado a las redes y digitalizado.

V. Capítulo 3. NORMAS RELEVANTES EN MATERIA DE CIBERSEGURIDAD EN LA LEGISLACIÓN CHILENA

Si se profundiza de forma acentuada en la legislación nacional chilena, hay normas relevantes a destacar que intervienen en al ámbito de ciberseguridad en Chile, dentro de las cuales podemos destacar[82]:

V.1 Constitución Política de la República

a) **Artículo 8,** en correspondencia a la transparencia pública.

b) **Artículo 19,** que contempla un catálogo de derechos fundamentales donde son especialmente relevantes: N°2, igualdad ante la ley; N°3 y 7, relativos al debido proceso y seguridad individual; N°4 y 5, sobre protección de la vida privada e inviolabilidad de las comunicaciones; N°12, que garantiza la libertad de expresión y de información; y N°24 y 25, relativos a la propiedad y libertad de creación.

[81] BEJIDE. J. (2023). *Ciberataques en Chile. Una amenaza virtual, pero real.* Diario El Mostrador. Consultado el 24 de Marzo de 2023. Recuperado de: https://www.elmostrador.cl/noticias/opinion/columnas/2023/03/05/ciberataques-en-chile-una-amenaza-virtual-pero-real/.
[82] MINISTERIO DE INTERIOR Y SEGURIDAD PÚBLICA (2017). Op. Cit. Pág. 30-32.

c) **Artículo 24,** que otorga a quien ejerza la Presidencia de la República la autoridad para conservar el orden público en el interior y la seguridad externa de la República, además de las normas que regulan las facultades de otros poderes y órganos del Estado.

d) **Artículos 39 y siguientes,** que regulan situaciones específicas que afectan el normal desenvolvimiento del Estado.

V.2 Leyes

a) **Ley N°19.913,** crea la unidad de análisis financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos: regula algunas medidas de investigación y vigilancia que, tal como en el caso Código Procesal Penal, pueden afectar la vida privada o inviolabilidad de las comunicaciones de sus destinatarios, y por ende la confidencialidad de su información, debido a lo también en este caso la ley exige una autorización judicial aparejada al cumplimiento de los requisitos legales del caso.

b) **D.L. N°211,** ley de Defensa de la Libre Competencia. Ley que autoriza la práctica de diligencias intrusivas en casos específicos, que se regulan en los mismos términos ya expuestos.

c) **Ley N°19.974,** sobre el Sistema de Inteligencia del Estado, conlleva a la creación de la Agencia Nacional de Inteligencia: en el marco de la recolección de antecedentes de inteligencia, esta ley regula la práctica de procedimientos especiales de obtención de información, que deben efectuarse con orden judicial previa y una serie de otros resguardos legales que limitan la obtención y uso de esta información.

d) **Ley N°21.459,** tipifica figuras penales relativas a la informática: dentro de los ciberdelitos, existe una subcategoría relativa a la afectación de los componentes lógicos del ciberespacio (programas de computación, sistemas informáticos, bases de datos), que se denominan delitos informáticos.

e) **Ley N°20.009** sobre Extravío, Robo o Hurto de Tarjetas de crédito y débito

f) **Ley N°18.168,** ley general de telecomunicaciones: esta ley regula el marco jurídico del sector de las telecomunicaciones en el país, que proveen de infraestructuras físicas y lógicas claves para el desarrollo del ciberespacio nacional. Dentro de sus disposiciones, destaca la protección de la confidencialidad e integridad

de la información mediante la tipificación de delitos de interceptación no autorizada (art. N°36B letras b y c). Cobran también especial relevancia para la ciberseguridad del país dos modificaciones recientes, correspondientes a la ley N°20.453, que consagra el principio de neutralidad en la red para los consumidores y usuarios de internet, que regula las medidas de gestión de red que puede adoptar un prestador de servicios de Internet, junto con establecer un deber de confidencialidad; y la ley N°20.478, sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones, promulgada tras el terremoto que afectó a Chile año 2010, y que como su nombre señala, establece medidas que permiten mantener la continuidad de las telecomunicaciones en el país y, con ello, la disponibilidad de la información contenida en el ciberespacio.

g) **Ley N°19.799,** sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma: regula el uso de documentos electrónicos en el país y, con ello, mecanismos para asegurar la integridad y confidencialidad de la información, mediante el uso de mecanismos de firma digital, junto con un sistema que garantice el apropiado funcionamiento de quienes prestan estos servicios.

h) **Ley N°20.285,** sobre acceso a la información pública: crea un régimen de transparencia para las actividades del Estado, con obligaciones de transparencia activa, que debe efectuarse a través del sitio web de cada organismo público afectado; y pasiva, consistente en los datos que puede requerir cualquier persona a estos organismos, en la medida que no afecte otros derechos e intereses establecidos en la ley, como la seguridad del Estado o la privacidad de terceros, de manera tal que no se afecte la confidencialidad de la información en juego.

i) **Ley N°19.927,** modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de delitos de pornografía infantil.

j) **Ley N°19.628,** sobre protección de la vida privada: establece un conjunto de principios y derechos relativos al manejo de datos personales en el país que puede exigir un titular de datos personales a quien posea o administre un registro de los mismos, junto con reglas de aplicación general para el manejo de datos personales por el sector público y privado, en torno al resguardo de la confidencialidad de esa información.

k) **Ley N°17.336,** sobre propiedad intelectual.

l) **Ley N°19.880,** establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del estado.

m) **Ley N°20.478,** sobre recuperación y continuidad en condiciones críticas y de emergencia del sistema público de telecomunicaciones.

V.3 Decretos

a) **D.S. N°83 de 2005,** aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos: este decreto, desarrollando lo establecido en la ley N°19.799, establece una norma técnica aplicable a la administración pública, respecto de la seguridad y confidencialidad de los documentos electrónicos, y con ello, también de su infraestructura de la información, basada en el estándar ISO 27.000 y, junto con ello, estableciendo medidas administrativas como la creación de comités de la seguridad de la información en cada servicio público. Complementa a este decreto el D.S. 93 de 2006, que aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios, y que como su nombre describe, regula medidas orientadas a prevenir la recepción de SPAM en las casillas electrónicas de la administración del estado.

b) **D.S. N°1.299 de 2004**, establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas: este decreto, teniendo como antecedente la ley de presupuestos para el año 2005 y el D.S. 5996/1999, consolida una intranet denominada Red de Conectividad del Estado, en la que deberán interconectarse una serie de ministerios y organismos públicos. Esta red centraliza el acceso a Internet y debe cumplir con estándares técnicos de seguridad acordes con los estándares del IEEE e ISO.

c) **D.S. N°1 de 2015,** aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado: actualiza las normas técnicas para los sitios web de la administración del Estado, regulando condiciones de confidencialidad, disponibilidad y accesibilidad de la información contenida en dichos sitios, todas condiciones centrales para la ciberseguridad.

d) **D.S. N°533 de 2015,** crea comité interministerial sobre ciberseguridad: crea un Comité interministerial con el objetivo de preparar una propuesta de Política Nacional de ciberseguridad, del que forma parte el presente anexo.

e) **Decreto N°83 de 2017,** promulga el Convenio sobre la Ciberdelincuencia.

f) **Decreto N°273 de 2022,** establece obligación de reportar incidentes de ciberseguridad.

V.4 Convenio de Budapest.

A escala de países, de forma transversal e internacional, para hacer frente a los delitos informáticos, se suscribió un tratado que busca frenar el avance y realización de aquellos ilícitos. El primer tratado global que aborda el tópico de la ciberseguridad, suscrito y ratificado por Chile, al igual que un gran número de países a escala internacional, es el *"Convenio sobre la Ciberdelincuencia"* (en adelante Convenio de Budapest). Chile se suscribió a él con fecha 23 de noviembre de 2001, y entró en vigencia en la legislación de Chile el 1 de Julio del año 2004.

Para desengranar de manera más técnica en el *"Convenio de Budapest"*, según establece su Preámbulo, es necesario mencionar que tiene por fin *"incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos"*[83], mediante *"una cooperación internacional reforzada, rápida y eficaz en materia penal"*[84].

Para cumplir lo mencionado en el preámbulo, el convenio en su núcleo contiene dos ámbitos específicos. Uno sustantivo que trata los delitos informáticos y uno procesal, con especial atención a las medidas de investigación y cooperación internacional en la persecución de estos delitos.

[83] CONVENIO SOBRE LA CIBERDELINCUENCIA. Preámbulo. Disponible en: https://rm.coe.int/16802fa403.
[84] Ibídem.

V.4.1 Ámbito sustantivo

En el ámbito sustantivo, se destaca la regla general de los tipos penales que se prevén en el convenio, donde se incluyen, como elemento subjetivo del tipo, que se trate de acciones deliberadas e ilegítimas, excluyendo con ello las conductas culposas y el dolo eventual[85].

La Sección 1 del Capítulo II (Derecho penal sustantivo) comprende las disposiciones relativas a los delitos y otras disposiciones pertinentes relativas a los delitos informáticos o delitos relacionados con el uso de computadoras. Primero, hay definición de 9 delitos agrupados en 4 categorías diferentes y luego analiza las obligaciones y sanciones asociadas. Se precisa los siguientes delitos: **acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[86].**

V.4.2 Ámbito adjetivo o normas procesales

El convenio prevé medidas de investigación y cooperación en el ámbito procesal, las que alcanzan no sólo los tiempos penales previstos en su texto, sino cualquier otro delito cometido por medio de un sistema informático[87].

El alcance del Capítulo II, Sección 2 (Procedimiento) del convenio, va más allá de los delitos definidos en la Sección 1 y cubre cualquier delito cometido utilizando un sistema informático o evidencia en formato electrónico. En primer lugar, establecer los términos y garantías comunes que se aplican a todas las facultades procesales contenidas en aquel capítulo. A continuación, establece las siguientes facultades procesales: **conservación rápida de datos informáticos almacenados; conservación y revelación parcial rápidas de los datos relativos al tráfico; la orden de presentación; el registro y la confiscación de datos informáticos almacenados; la obtención en tiempo real de datos relativos al tráfico, y la**

[85] DONOSO,L. REUSSER, C. (2021). Derecho Informático. Academia Judicial. Pág 108.
[86] CONVENIO SOBRE LA CIBERDELINCUENCIA. (2001*).* Op. Cit. Pág. 6.
[87] DONOSO,L. REUSSER, C. (2021). Op. Cit. Pág. 108.

interceptación de datos relativos al contenido. Al final de la sección del Capítulo II, se incluyen disposiciones en materia de jurisdicción[88].

Si bien el convenio no define exactamente en torno a que se comprende como ciberdelincuencia ni expresa directamente de modo literal sobre los delitos informáticos, en Chile, el Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el *"Convenio de Budapest",* nos da señales de lo que se puede entender por ciberdelincuencia, gracias a las normas contenidas en las declaraciones del convenio, como de igual forma lo contemplado en las reservas que se le hicieron al mismo.

En efecto, en torno a las *"Declaraciones al Convenio sobre la Ciberdelincuencia",* el Decreto delibera que:

> a) La República de Chile declara que **exigirá una intención delictiva determinada en el sujeto activo** para penar las acciones descritas en los artículos 2 y 3 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el artículo 2 de la ey N° 19.223 (en la actualidad derogada y reemplazada por la ley 21.459) sobre delitos informáticos[89].
>
> b) La República de Chile declara que **exigirá un ánimo fraudulento que produzca un perjuicio a terceros** para penar las acciones descritas en el artículo 7 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el artículo 197 del Código Penal[90].

El artículo 2 del convenio, el cual se refiere al **"acceso ilícito"**, obliga a la tipificación como delito el acceso deliberado e ilegítimo a todo o parte de un sistema informático. En este sentido, cabe señalar que al Estado se le puede exigir sancionar los delitos cometidos violando la seguridad, con el fin de obtener datos informáticos o con otro fin delictivo, o del mismo modo, con un sistema informático conectado a otro de la misma naturaleza.

[88] CONVENIO SOBRE LA CIBERDELINCUENCIA. (2001). Op. Cit. Pág. 6.
[89] MINISTERIO DE RELACIONES EXTERIORES . *Decreto 83.* Diario Oficial de la República de Chile. Santiago, Chile, 28 de Agosto de 2017. Pág. 1.
[90] Ibídem.

Ahora bien, dentro de otros artículos relevantes en el *"Convenio de Budapest"* encontramos el artículo 3, en el cual se desglosa la **"interceptación ilícita"**. En ella se coacciona exigiendo a los Estados partes, que tipifiquen como delito la interceptación deliberada e ilegal de datos informáticos por medios técnicos, la transmisión no pública a un sistema informático que tenga lugar o se lleve a cabo en un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, pudiendo coaccionar a los Estados miembros, a que el delito se cometa en conexión con un sistema informático conectado a otro sistema informático, o con intención delictiva.

Por otra parte, con relación al artículo 7 del convenio, se obliga a los Estados a tipificar el "delito de falsificación informática", consistente en la introducción, alteración, borrado o eliminación consciente e ilegal de datos informáticos que generan datos falsos con la intención de utilizarlos como datos genuinos para fines legales, con independencia de que los datos sean legibles o no, pudiendo mediante la coacción, exigir a los Estados parte, que exista una intención dolosa o delictiva similar para que pueda considerarse que existe responsabilidad penal. Para efectuar esa tipificación, el decreto promulgado, declara que Chile exigirá un ánimo fraudulento que produzca un perjuicio a terceros, conforme lo requiere el artículo 197 del Código Penal, que a su vez se refiere a la falsificación de instrumento privado con perjuicio de terceros.

Efectuando un parangón entre la legislación chilena y el convenio, desde un punto positivo, se puede establecer que Chile ha ido un paso más allá del *"Convenio de Budapest"* porque localmente, a modo de ejemplo, se regula la "**receptación de datos informáticos"** en el artículo 6 de la ley 21.459, delito que no se encuentra contemplado en el convenio.

De igual forma, en la ley 21.459 se regula la "**hipótesis de facilitación de medios".** Hay un desglose del acceso ilícito que no es exactamente como el convenio, en el fondo sanciona el mero acceso ilícito, como de igual forma, el acceso ilícito que involucra conocimiento de los datos. Dicho esto, a modo de especulación, se puede establecer que al final lo que se va a provocar, es que se aplique mucho más el mero acceso ilícito, dado que de lo contrario debe involucrar espacios probatorios mayores.

Cabe enunciar que, en beneficio de la investigación y persecución de los delitos informáticos, el 12 de mayo del 2022 Chile, junto con los otros 21 países miembros del

“Convenio de Budapest”, firmaron el segundo protocolo de este importante marco legal, que tiene como fin mejorar la cooperación internacional y la compartición de pruebas electrónicas de ciberdelitos. Este nuevo acuerdo proporciona herramientas para una mayor cooperación e intercambio de pruebas electrónicas (por ejemplo, cooperación directa con proveedores de servicios de Internet y registros, métodos eficientes para obtener información de usuarios y datos de tráfico, o cooperación inmediata en situaciones de emergencia e investigación conjunta). El uso de estas herramientas se regirá por las garantías de los derechos humanos y el estado de derecho, incluidas las garantías de protección de datos personales. La actualización de este protocolo es particularmente importante debido a la evolución del cibercrimen, el desarrollo de la tecnología y los desafíos que se enfrentan día a día.

A modo de concluir este capítulo, es loable enunciar, que si bien el convenio se refiere a la “ciberdelincuencia” y a los delitos informáticos, sin definirlas, sus artículos 2, 3 y 7, se obliga a los Estados parte, a tipificar en sus legislaciones, sobre los expresado en aquellos artículos mencionados. En otras palabras, el convenio introduce una clasificación de conductas en la que los medios o elementos informáticos **suelen estar sujetos al objeto de la conducta típica y no simplemente a los medios para cometer un delito.**

Un detalle importante a remarcar, y en el cual es necesario que se perfeccione la legislación actual a futuro, es que Chile se compromete a tipificar aquellos delitos mencionados, sin embargo, exige en ellos **una intención delictiva determinada en el sujeto activo** (artículos 2 y 3 del convenio) **y ánimo fraudulento que produzca un perjuicio a terceros** (artículo 7 del convenio).

VI. Capítulo 4. LEY 21.459

VI.1 Tipos penales de la ley 21.459

Una de las principales novedades de la ley N° 21.459 constituye la modernización de los tipos penales para adecuarlos a las nuevas formas de comisión de los delitos informáticos,

en consideración a los nuevos riesgos y ataques sobre bienes jurídicos relevantes que no estaban contemplados en la anterior ley N° 19.223[91].

Por lo tanto, entre otras cosas, es posible apreciar el establecimiento de tipos penales destinados a sancionar expresamente el acceso ilícito a un sistema de información. En la ley N° 21.459 (no se requiere un propósito especial, artículo 2), el ataque a la integridad de un sistema informático o para afectar su normal funcionamiento (artículo. 1), así como también la interceptación ilícita de información (artículo 3) y, en su caso, el ataque a la integridad de estos (artículo 4). A su vez, se incluye expresamente la figura de fraude informático (artículo 7), que permitirá sancionar las actividades fraudulentas cometidas por medios electrónicos, antes sólo parcialmente dirigidas a figuras fraudulentas generales (artículo 7). También se sanciona de manera separada la falsificación informática con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (artículo 5)[92].

Entre los nuevos delitos, se incluye la "recepción de datos informáticos" (artículo 6), donde se sanciona a quien venda, transfiera o almacene datos informáticos bajo cualquier título, conociendo o no pudiendo menos que tener conocimiento de la procedencia ilícita, es decir, proveniente, de alguno de los delitos tipificados en la ley. Sumado a ello, se incluyen cifras por mal uso de equipos (artículo 8).

Adicionalmente, se incluye la figura de cooperación eficaz como una atenuante de la responsabilidad, es decir, permitir la reducción de las sanciones impuestas a quien proporcione información para establecer los hechos, identificar a los responsables o impedir o impedir la ejecución de los delitos (artículo 9).

Al contrario, se contempla circunstancias agravantes a los que delinquen, abusando del cargo de confianza en la administración del sistema informático o custodio de los datos en el sistema informático. También se considera una circunstancia agravante, el cometer el delito abusando de las debilidades, la confianza, el desconocimiento de niños, niñas, adolescentes o adultos mayores (artículo 10). Asimismo, si se afecta y/o interrumpe la prestación de los

[91] ALDONEY, R. ALBERTZ, P. & ALCAÍNO E. (2022). *Nueva Ley de Delitos Informáticos: aspectos penales y de compliance.* Estudio Jurídico Carey. Consultado el 17 de Marzo de 2023. Recuperado de: https://www.carey.cl/nueva-ley-de-delitos-informaticos-aspectos-penales-y-de-compliance/.
[92] Ibidem.

servicios públicos o el curso normal del proceso electoral de conformidad con la ley N° 18.700, se considerará de igual forma, una circunstancia agravante.

Por otra parte, **se contemplan igualmente medidas especiales de investigación, como el uso de agentes encubiertos** (artículo 12).

La nueva ley también establece disposiciones según las cuales el Ministerio Público, **con o sin autoridad judicial**, puede solicitar información, según las diversas situaciones que se encuentran reguladas, a las empresas prestadoras de servicios de comunicaciones, los cuales no sólo están obligados a proteger la información, sino que también están sujetos. a la confidencialidad, cuya violación será sancionada de conformidad con el artículo 36 B de la ley N° 18.168. De forma similar, establece estándares para la evidencia electrónica.

Cabe señalar que los delitos informáticos antes señalados están incluidos en el catálogo básico de delitos de la ley N° 20.393, lo que dará lugar a la responsabilidad penal de las personas jurídicas. En este sentido, las empresas y personas jurídicas deben identificar las actividades o procesos rutinarios o irregulares de la entidad, que crean o aumentan el riesgo de cometer delitos cibernéticos e implementar protocolos, políticas y procedimientos específicos para prevenir la ocurrencia de los delitos antes mencionados. Para estos efectos, deberán realizar estudios de riesgo para cubrir estos nuevos escenarios de riesgo y actualizar sus respectivas matrices de riesgo y modelos de control de prevención de delitos.

La nueva ley también define el llamado "hacking ético", **eximiendo de responsabilidad penal** a quienes accedan a los sistemas informáticos con **autorización expresa de su titular**, en relación con la investigación de vulnerabilidades o la mejora de la seguridad informática (artículo 16)[93].

Todos los delitos informáticos contemplados en esta ley se añadirán al catálogo anterior de delitos de lavado de activos en conformidad con la ley N° 19.913, que crea la Unidad de Análisis Financiero y se modifican diversas normas relacionadas con el blanqueo y lavado de activos.

[93] Ibidem.

Dentro de los delitos que contempla esta nueva ley se destacan[94]:

- Acceso ilícito.
- Interceptación ilícita.
- Ataque a la integridad de los datos informáticos.
- Falsificación informática.
- Receptación de datos informáticos.
- Fraude informático.

La ley en comento modifica los siguientes cuerpos legales a considerar[95]:

⇒ Ley N° 19.223, tipifica figuras penales relativas a la informática.

⇒ Código Procesal Penal.

⇒ Ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos

⇒ Ley N° 18.168, General de Telecomunicaciones.

⇒ Ley N° 20.393, Establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica.

Ahora bien, haciendo un sucinto contraste entre la ley N° 21.459 y la anterior ley N° 19.223, se puede detallar que:

Con respecto a la manipulación de datos con ánimo de lucro y que acarrea un perjuicio patrimonial para la víctima, esa figura no la contemplaba la ley N° 19.223, pero en la 21.459 si, se regula expresamente.

En la ley N° 19.223, La hipótesis de acceso no autorizado a información contenida en sistemas computacionales, ofrecía problemas al momento de aplicarse, tal es el exigir la concurrencia de un elemento subjetivo adicional (ánimo de apropiación, uso o conocimiento), cuestión que se aborda de forma más completa en la ley N° 21.459.

[94] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. (2022). Op. Cit.
[95] BARRERA, V. (2022). *Se publica Ley que moderniza normas sobre delitos informáticos.* Thomson Reuters. Consultado el 2 de Diciembre de 2022. Recuperado de: http://www.laleyaldia.cl/?p=16162.

Viéndolo desde una perspectiva general, la ley N° 19.223 no legislaba en sus artículos expresamente una gran variedad de hechos ilícitos de trascendencia en la actualidad, como el phishing, hacking, fraude informático, asociación para cometer delitos informáticos, actos preparatorios. Eran únicamente 4 artículos que tipificaban figuras penales relativas a la informática de manera genérica, no abordando ni técnica ni específicamente una variedad de delitos que hoy en día existen. La ley N° 21.459 entrega una mayor descripción de las figuras delictivas y sanción de estos delitos, entregando mayor certeza jurídica, para efectuar de mejor forma la persecución delictiva[96].

VI.2 Análisis dogmático de la ley 21.459

La ley N° 21.459 regula diversos tipos penales, tales como; **ataque a la integridad** de un sistema informático, **acceso ilícito** a un sistema informático, **interceptación ilícita** de información, **falsificación informática**, **receptación de datos informáticos**, entre otros[97].

Se incluye, de igual forma, la figura de **fraude informático** que castiga a quienes perjudican a otros en beneficio propio o de un tercero mediante la manipulación de los sistemas informáticos mediante diversas acciones como introducir, alterar, corromper o borrar datos informáticos. Estos delitos se agregaron al catálogo de delitos procedentes por lavado de dinero de conformidad con la ley N° 19.913, que creó la Unidad de Análisis Financiero, y modificó diversas disposiciones sobre blanqueo y lavado de activos, la cual es fuente de responsabilidad de las personas jurídicas.

Es necesario recordar que la **ley N° 20.393** sobre Responsabilidad Penal de las Personas Jurídicas, atribuye responsabilidad a estas, en cuanto al incumplimiento de los deberes de dirección y supervisión que tienen los sujetos. Es decir, aquellos relacionados con la Alta Dirección o Gerencia de una compañía[98].

[96] CAVADA, J. (2015). *Delitos Informáticos. Chile y legislación extranjera*. Biblioteca del Congreso Nacional. Pág. 39- 41. Disponible en: Https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/22170/3/Delitos%20Inform%C3%A1ticos%202015.pdf.
[97] Ley 21.459. Artículos 1 al 7.
[98] Ley 20.393. Artículo 3.

En suma, la **ley N° 21.459** está segmentada en tres títulos denominados. **Título I**, de los delitos informáticos y sus sanciones, **Título II,** del procedimiento, y **Título III,** disposiciones finales.

Uno de los artículos que causa atención, es el n°9 correspondiente al **Título I,** el cual señala:

"Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la **cooperación eficaz** que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley. O permita la identificación de sus responsables. O sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

Se entiende por **cooperación eficaz** el suministro de datos o informaciones precisas, verídicas y comprobables, que contribuyan necesariamente a los fines señalados en el inciso anterior"[99].

Por su parte, en el Título III, llama la curiosidad por parte del legislador las definiciones que se establece para efectos de esta ley, en donde se entenderán por:

a)Datos informáticos. Toda representación de **hechos, información o conceptos** expresados en cualquier forma que se preste a tratamiento informático. Incluidos los programas diseñados para que un sistema informático ejecute una función.

b) Sistema informático. Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

c) Prestadores de servicios. Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático y

[99] Ley 21.459. Artículo 9.

cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo[100].

Ahora bien, examinando el articulado de la ley N° 21.459, artículos importantes a destacar son:

Dentro d**el artículo 1** se detalla lo relacionado a que en **la medida que se prescinde de un actuar deliberado, también se prescinde del dolo directo.**

Se encuentra una omisión de referencia a la obstaculización en forma grave, esto sirve para fundamentar que basta una obstaculización que no sea grave para aplicar el tipo penal, no obstante, era una exigencia que era prescindible porque no podría a idéntico resultado aplicando solamente criterio de imputación objetiva, para lograr que se castigue la conducta, porque esta tiene que tener cierta entidad.

En el **artículo 4** en torno a la figura del **ataque a la integridad de los datos informáticos** se dice que es necesario que se cause un daño grave al titular de esos mismos datos. En esta parte se abordó explícitamente esta cláusula relativa a la identidad del comportamiento. Además, se agrega la cláusula en el sentido que la conducta debe ser realizada de manera indebida. Es una cláusula que causa dudas, dado que se tendría que responder la pregunta relativa a cuando la conducta se efectúa de forma indebida. Visto esto, es algo que se va a tener que solucionar en torno a la interpretación doctrinal.

En relación al **espionaje informático**, se incluye en esta ley una referencia explícita a un elemento, el cual tiene que ver con la realización del comportamiento del espionaje sin autorización de la persona que es titular del sistema o de los datos en el **artículo 2** de la ley N° 21.459. Desde ese punto de vista se podría llegar a la conclusión de que esta referencia es algo que se explicita, a pesar que la doctrina[101] ya entendía que estaba incluida en el tipo penal. Luego se hace referencia a barreras técnicas o tecnológicas, esto puede resultar positivo dado que da certeza al aplicar el tipo penal y justamente aplicarlo en los casos en que

[100] Ibidem. Artículo 15.
[101] WINTER ETCHEVERRY, J. (2013). *Elementos típicos del artículo 2° de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 9238-12.* Revista de Ciencias Penales. Pág. 278-282. Disponible en: http://revistadecienciaspenales.cl/wp-content/uploads/2019/02/Corte-Suprema-6.
-8.pdf.

es claro que el titular de la información quiere excluir a terceros del acceso a los datos o sistema de que se trata.

Se encuentra una hipótesis de acceso ilícito como lo nomina la ley, porque básicamente se contemplan dos figuras, no una. Una que tiene que ver con medio hacking y otra que tiene que ver con la idea de realizar el comportamiento con el ánimo de apoderarse o utilizar la información contenida en el sistema informático. Esta segunda modalidad tiene el problema que exige este ánimo especial, por lo cual, es difícil aplicar desde este punto el tipo en la práctica, esto porque si no se acredita presencia de ese ánimo, cae la posibilidad de imponer la sanción. Lo anterior es un elemento que podría augurar una aplicación mucho más intensa de la figura de hacking o mero hacking, puesto que, como en esa figura solamente se exigía un acceso ilícito sin que se demande ánimo especial, una persona podía esperar que se aplicara de manera subsidiaria, o que no se logre acreditar todos los elementos de segunda modalidad, entonces va a tener aplicación probablemente la primera. Sin embargo, es algo que hoy no se logra porque en la actual legislación nacional no contamos con una figura de hacking simple o mero hacking puniblemente sancionable.

Una de las cuestiones trascendentes de este nuevo cuerpo legal es que viene a establecer **agravantes y atenuantes específicas**. En ese marco, da una impresión de que hay una legislación especializada, la cual permite tomar en consideración algunas circunstancias que pueden ser, aligerar la responsabilidad o incrementarla.

En relación a lo expuesto, las reglas procesales son fundamentales para que, en el fondo, toda la aplicación funcione bien. Es de común conocimiento que la forma del derecho es la que determina finalmente hacer exigible la responsabilidad.

La modificación del Código Procesal Penal es un punto a destacar de igual manera, esto en torno a la interceptación de las comunicaciones, implica un gran avance. La preservación provisoria de datos es una de las cuestiones que ha sido motivo para que esta ley haya resultado particularmente un asunto de interés en el mundo corporativo, porque se viene a unir al catálogo de conductas donde eventualmente va a existir responsabilidad penal de las personas jurídicas. Es necesario que las compañías estén atentas de cuál es el riesgo que se va a evitar, cuáles son aquellos que están dispuestos a tolerar, cuáles están en condiciones de mitigar y qué tipo de riesgo en el fondo no tienen ninguna chance de observar

para finalmente contratar un seguro. Dicho lo anterior, ese tipo de conducta desde las organizaciones privadas es súper determinante al momento de aplicar las reglas que dicen relación con **responsabilidad penal de la persona jurídica**, por lo tanto para el interés del mundo corporativo, es de suma importancia prestarle atención.

Otro punto es, en torno al delito, donde se preocupa de establecer una figura básica, que puede cometer cualquier sujeto, y una figura agravada que debe cometer un funcionario público, esto se regula de forma expresa en el artículo 10 de la ley N° 21.459.

El problema que puede generar esta figura radica especialmente en su vinculación con la hipótesis tradicionales de falseado documental, que están reguladas en el Código Penal[102], y que en los últimos años ha ido ganando cierto terreno la tesis que planteaba una interpretación amplia del concepto documento, entendiendo por tal a cualquier soporte que es capaz de fijar una determinada declaración. De acuerdo con esta interpretación amplia, entonces sería perfectamente posible cometer una falsedad tradicional afectando un documento electrónico. No obstante, si se regula expresamente una supuesta falsedad informática en la nueva ley, ello podría abonar la tesis de que las falsedades tradicionales no pueden tener como objeto un documento electrónico, pues para ello estaría obviamente este nuevo delito. Pero junto con eso, esta regulación de la nueva ley de delitos informáticos podría incidir incluso en la interpretación de otros delitos de la parte especial. Pensemos, a modo de ejemplo, en la violación de correspondencia, delito a propósito del cual uno también veía que se planteaban una interpretación amplia de esta idea de correspondencia, no solamente a la que se lleva a cabo mediante papel, sino que también la que es propiamente electrónica. Entonces, en resumen, ubicar una hipótesis específica de falsedad en esta ley, puede generar una dificultad respecto de las falsedades tradicionales, pero también respecto de otros delitos de la parte especial que tienen por objeto material, algo que podría entenderse como un documento en términos amplios.

En torno al acceso ilícito del artículo 2 de la ley N° 21.459, probablemente es uno de los temas en donde, por una parte, se regula una hipótesis de mero acceso al sistema y otra que exige ánimo de apoderarse o usar la información. Curiosamente, no alude al ánimo de conocer la información como lo hacía el artículo segundo de la ley N° 19.223, lo que podría

[102] Código Penal de Chile. Artículo 193.

llevar a preguntarse si es que, ese conocimiento es un requisito de la hipótesis básica, pero eso es algo que va a quedar para la interpretación doctrinaria y jurisprudencial.

De todas maneras, la exigencia del ánimo referido puede provocar el mismo problema que provocaba anteriormente, es decir, que la no acreditación en juicio de dicho ánimo genere que el tipo penal no se pueda aplicar. Sin embargo, a contrario sensu, la gran ventaja con la que se va a contar con la ley N° 21.459 es que si no se logra acreditar ese ánimo, muy probablemente va a tener aplicación el mero acceso ilícito. Entonces, desde ese punto de vista se cuenta con una figura de respaldo, que no se contaba para la aplicación de acuerdo a la ley N° 19.223.

Ahora bien, se debe celebrar la consagración explícita de la superación de barreras técnicas o medidas tecnológicas de seguridad, la cual era una cláusula que parte de la doctrina entiende implícita en las hipótesis de acceso lícito de espionaje informático[103]. Es positivo que se incluya explícitamente, porque nos da certeza respecto de la pretensión del titular del sistema o de los datos de excluir a terceros, en relación con acceder a dicho sistema o a dichos datos.

Abordando de manera breve, un delito que como tal no se contempla en el convenio, es el relacionado con el tipo de receptación de datos informáticos. La regulación de dicho delito resulta coherente con la tipificación de, por ejemplo, la receptación en materia de delitos contra la propiedad. Junto con la consagración de esta figura se añade una que tiene ciertos puntos de contacto con la receptación, la cual es la hipótesis que se contempla en la parte final del artículo séptimo dedicado al fraude informático y que es muy interesante en la ley N° 21.459. Cabe mencionar que es bastante expansiva, pero es una hipótesis que sanciona o que establece más bien penalidad para los efectos del artículo que regula el fraude informático. En consecuencia, se considerará que el autor al tener conocimiento o no pudiendo menos que conocer la ilicitud de la conducta descrita en el fraude informático, hace facilitación de los medios con que se comete el delito. Tanto la receptación como este último supuesto delictivo son ejemplos claros de regulación de comportamientos que buscan superar dificultades probatorias que se generan muy frecuentemente en la práctica, y que es una cuestión no

[103] MAYER LUX, L. & VERA, J. (2020). *El delito de espionaje informático: Concepto y delimitación.* Scielo. Consultado el 22 de Marzo de 2023. Recuperado de: ttps://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000200221.

solamente frecuente, en materia de fraude informático, sino que incluso de fraude en general[104].

A modo de ejemplo, pensemos en la situación que se encuentra una persona, la cual facilita su cuenta corriente para que a ella sea realizada una transferencia electrónica. Esa es una situación que provoca muchas dificultades en la práctica, porque es usual que no se pueda establecer un vínculo entre quien cometió el fraude tradicional o informático y quién tiene los fondos. Entonces, la persona que tiene el fondo puede expresar y decir que efectivamente tiene este dinero, pero cómo se prueba en definitiva que esa persona estaba concertada o estaba actuando como coautor de aquella que realizó el fraude propiamente tal. Esta hipótesis, entonces, va a permitir castigar a lo que algún sector de la doctrina denomina "las mulas"[105], que son aquellos sujetos que facilitan medios para operar como intermediarios de los fondos ilícitamente transferidos a través de Internet.

VI.3 Similitudes con el Convenio de Budapest

El texto de la ley N°21.459 por primera vez plantea lo que se podría denominar un catálogo completo de delitos informáticos, en sentido estricto, sobre delitos que se cometen en contra de sistemas informáticos. La regulación de delitos en muchos casos siguen el *"Convenio de Ciberdelincuencia de Budapest",* por ejemplo, promulgando el *"Decreto 83"* sobre la ciberdelincuencia[106].

Desde el punto de vista de las similitudes con el convenio hay que destacar, en primer lugar, la hipótesis de ataque a la integridad del sistema informático, como también la hipótesis de ataque a los datos, el acceso ilícito, y la interceptación ilícita. Además, por primera vez se cuenta con una ley que se haga cargo específicamente de la manipulación de datos que provoca un perjuicio patrimonial y es realizada con ánimo de lucro[107].

[104] MAYER LUX, L., & OLIVER CALDERÓN, G. (2020). Op. Cit.
[105] Ibidem
[106] PORTALES, M. (2022). *Nuevo Catálogo de Delitos Informáticos y Compliance Penal.* Círculo Inhouse. Consultado el 29 de Noviembre de 2022. Recuperado de: https://circuloinhouse.cl/compliance/nuevo-catalogo-de-delitos-informaticos-y-compliance-penal/.
[107] Ley 21.459. Artículo 1 al 4.

Ahora bien, otro asunto a destacar, es el tipo penal de abuso de dispositivos, que básicamente sanciona el hecho de poner a disposición de otros, dispositivos, programas, contraseñas, etcétera no creados para la Comisión de Delitos Informáticos.

Llama la atención, el ámbito de aplicación que se fijó para el delito, pues únicamente se alude al uso de los dispositivos para cometer los tipos regulados entre el artículo primero y el cuarto de la ley. En otras palabras, se refiere al ataque de la integridad del sistema de los datos, acceso ilícito e interceptación ilícita. Sin embargo, no hay una referencia explícita al abuso de los dispositivos respecto del fraude informático.

Otro elemento a recalcar que está contenido en la ley N° 21.459, es la consagración del abuso de dispositivos a propósito del delito del artículo 7 en la ley N° 20.009, que sanciona fraudes relacionados con tarjetas de pago y transacciones electrónicas ilícitas, que tienen puntos de contacto con el fraude informático. En lo que se refiere a este punto, es extraño que no se haya explicitado al estado informático dentro de ese listado de comportamientos. Esto podría provocar en la práctica que el abuso de dispositivos para cometer un fraude informático deba sancionarse indirectamente, de forma parecida a como lo que trata la ley N° 19.223 en relación con el fraude informático propiamente tal. Es decir, se necesitaría que uno tenga que recurrir a un abuso de dispositivos, por ejemplo, para imputar un acceso ilícito o un abuso de los dispositivos, o también, para imputar de un ataque a la integridad de los datos. Y luego, por esa vía indirecta, intentar lograr ese efecto que se habría logrado, si es que el legislador hubiese contemplado en el catálogo el artículo que se refiere específicamente al fraude informático.

Como última similitud de suma importancia a mencionar, es que la nueva ley de delitos informáticos, al igual que el convenio, regula también un supuesto de falla informática, donde básicamente implica falsificar datos informáticos[108].

VI.4 Facultades investigativas en torno a los delitos informáticos

Además, del avance de la generación de nuevos delitos, la normativa progresa enormemente desde una perspectiva procesal; ello puesto que la antigua ley nada señalaba al respecto. Esto cobra especial relevancia por el carácter transfronterizo que tienen estos

[108] Ibidem. Artículo 5.

delitos, unido a la posibilidad que puede ser cometido por un solo sujeto o una asociación de personas u organizaciones criminales, sin que cuenten obligatoriamente con conocimientos especializados en informática[109]. Por lo mismo, la incorporación de figuras como el **agente encubierto en línea[110]**, como los aspectos relativos a la **cadena de custodia de la evidencia de electrónica[111]**, es decir cómo se debe resguardar la información de un sistema informático para ser presentado en una investigación, se vuelven necesarias para resguardar los derechos de las personas.

La normativa modifica una serie de cuerpos legales, entre ellos el Código Procesal Penal (en adelante CPP), incluyendo la **figura de preservación provisoria de datos informáticos**, que se torna importante en investigaciones judiciales internacionales de alta complejidad en que se requiere acceder a la información con autorización judicial ubicada en otro país, siempre que se cuente, como se dijo con una autorización del juez competente. En el mismo sentido, se incorporan delitos informáticos que son base para configurar responsabilidad penal de las personas jurídicas según la ley N° 20.393. Por ejemplo, la obligación de informar sobre algunos sujetos obligados por la ley Nº 19.913 que crea la Unidad de Análisis Financiero (UAF). Para terminar este punto, cabe consignar que se hacen modificaciones a la ley General de Telecomunicaciones, agregando una sanción penal en caso de infracción a los deberes de reserva o secreto[112].

VI.5 Técnicas especiales de investigación en la ley 21.459 y recopilación de prueba.

Como se detalló a modo genérico en párrafos anteriores, la ley destinó un título particular (II), en el que se regulan ciertas técnicas especiales para la indagación de tales ilícitos. Dentro de la cuales encontramos las medidas de interceptación de comunicaciones privadas, otros medios técnicos de investigación y al establecimiento de agentes encubiertos. La cooperación eficaz también se podría considerar dentro de este grupo.

[109] Diario Financiero Deloitte. (2022). *Aspectos generales de la Ley de Delitos Informáticos (Ley N° 21.459).* Consultado el 4 de Octubre de 2022. Recuperado de: https://deloitte.diariofinanciero.cl/aspectos-generales-de-la-ley-de-delitos-informaticos-ley-no-21-459/.
[110] Ley 21.459. Artículo 12.
[111] Ibidem. Artículo 14.
[112] Ley 18.168. Artículo 36b, letra e.

Los delitos informáticos de la ley N° 21.459 están regulados como simples delitos, esto da motivo al legislador para que este haya decidido restringir el ámbito de aplicación de las técnicas en comento únicamente a los ilícitos penales más graves.

La introducción de una excepción a las reglas generales, se puede relacionar especialmente con lo compleja que resulta la investigación penal por la comisión de delitos informáticos, por ejemplo, en lo que respecta a la identificación de su autor o a la acreditación del elemento subjetivo[113].

Pese a que el legislador hace un reenvío a los artículos 222 a 226 CPP, cabe consignar, la regulación de manera expresa sobre las condiciones de procedencia de la interceptación de comunicaciones y de otros medios técnicos de investigación. Dicho lo anterior, se necesita que la investigación haga "imprescindible" la utilización de estas medidas para la persecución del delito, idea que derivaría del principio de prohibición de exceso[114].

Si se aborda sobre una diligencia intrusiva de investigación, el legislador estableció de manera expresa el presupuesto material para su procedencia, a saber, que existieren fundadas sospechas con argumentos basados en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los artículos 1, 2, 3, 4, 5 y 7 de la ley. Lo dicho con anterioridad conlleva una exigencia para el Ministerio Público, la cual es que previo a la solicitud que formule ante el Juez de Garantía, a fin de obtener la autorización judicial respectiva, se debe contar con antecedentes relativos a la existencia de un delito informático y a la intervención en dicho delito, de un modo penalmente relevante, de uno o más imputados. El estándar requerido es que baste con la concurrencia de indicios que permitan dar por establecida la existencia del hecho y de la intervención indicados[115].

Por otra parte, es cuestionable (dependiendo la perspectiva de política a aplicar que tenga cada persona), que el legislador, al regular el presupuesto de aplicación de tales diligencias intrusivas, se refiera tanto a la comisión como a la preparación del hecho, dado que

[113] MAYER LUX, L & VERA, J. (2022). *La nueva ley de delitos informáticos. Vol. XLVIII. N°3.* Revista de Ciencias Penales. Pág. 321. Disponible en: http://revistadecienciaspenales.cl/wp-content/uploads/2023/04/RCP-3-2022-Final-273-342.pdf.
[114] HORVITZ, M. y LÓPEZ, J. (2017). *Derecho Procesal Penal Chileno*, *Tomo I*, reimpresión de la 1a ed. Santiago: Editorial Jurídica de Chile. Página 529 con referencias ulteriores.
[115] MAYER LUX, L & VERA, J. (2022) Op. Cit. Pág. 322.

se podría habilitar a la autorización de esas diligencias cuando los delitos informáticos respectivos se encuentren en la etapa de los actos preparatorios.

El legislador excluyó de la procedencia de estas técnicas especiales de investigación al delito previsto en el artículo 8 de la ley N° 21.459[116], el cual es el único que sanciona formas de preparación de delitos informáticos como tipo penal autónomo. Esto trae como consecuencia que a pesar de la referencia a la preparación que prevé la norma en comento, el Juez de Garantía solamente podrá acceder a la solicitud del Ministerio Público en el evento de que este demuestre que el hecho investigado se encuentra a lo menos en fase de tentativa[117].

Una contradicción a expresar, es que incluir a los actos preparatorios en el presupuesto de aplicación de dichas diligencias iría en contra de la proporcionalidad que se encuentra por detrás de la exigencia, ya que está señalado que la investigación de los respectivos delitos hace imprescindible la utilización de esas técnicas.

En torno a la utilización de otros medios técnicos de investigación, ante el silencio de la ley N° 21.459, se debe interpretar que dicha medida se refiere a aquella regulada en el articulado del Código Procesal Penal, disposición que **posibilita a petición del Ministerio Público que el Juez de Garantía ordene la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos como prueba**. El juez también podrá disponer la grabación de comunicaciones entre personas presentes[118].

Como ya se mencionó, esta debida diligencia en materia de delitos informáticos tiene una especificidad en que no necesariamente tiene que ser utilizada para cometer un hecho delictivo merecido, a diferencia de lo que establece como regla general el artículo 226 del Código Procesal Penal. Esto es así porque si bien la nueva ley hace referencia a los artículos 222, 223, 224, 225 y 226 del Código Procesal Penal, también indica que tales procesos se

---

[116] Ley 21.459. Artículo 8, relacionado al abuso de dispositivos. *"El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales."*

[117] HORVITZ, M. & LÓPEZ, J. (2003) *Derecho Procesal Penal Chileno*. Tomo I. Santiago: Editorial Jurídica de Chile. Pág. 528.

[118] Código Procesal Penal Chileno. Artículo 226.

aplican con carácter general a los delitos informáticos más graves previstos en la ley N° 21.459.

Ahora, en cuanto al agente encubierto, el artículo 12, párrafo 3, de la ley N° 21.459, permite que la policía actúe en esa calidad, bajo una identidad falsa y mantenga correspondencia en canales cerrados de comunicación. De acuerdo a lo señalado, la ley prevé "agentes encubiertos cibernéticos" o "ciber agentes encubiertos", también conocidos por los legisladores como "agentes encubiertos en línea" (artículo 12 inciso 3), cuyos sujetos de actuación se realizarán a través de sistemas informáticos, especialmente a través de Internet.

Es concebible que los agentes encubiertos ingresen "físicamente" a las organizaciones criminales con el objetivo de cometer delitos informáticos, no obstante, la ley prevé lo contrario para los agentes encubiertos en el ámbito informático, lo que debe interpretarse restrictivamente, pues nos encontramos ante medidas que restringen derechos fundamentales, según el artículo 5 del CPP, estas medidas no pueden ser aplicadas por analogía. Por lo tanto, se descarta la intervención física de ciberagentes encubiertos. Nuevamente, ante la ausencia de otras normas que amplíen la participación policial en las investigaciones de delitos informáticos, el referido sería el ámbito limitado para que los agentes encubiertos cibernéticos expresen reconocimiento legal.

En principio, en nuestro ordenamiento jurídico, para investigar la comisión de delitos informáticos, en el marco de ciber patrullas intrusivas, la única forma eficaz de recabar información es a través del perfil de agentes encubiertos. Por lo tanto, la información de las patrullas de la red realizadas fuera de los límites de los agentes encubiertos de la red puede dar lugar a la posibilidad de pruebas ilegales. Esto puede ocurrir, si las patrullas cibernéticas acceden a los sistemas informáticos únicamente con fines de control o vigilancia, sin que se conozcan conductas ilegales ni procesos penales. Además de lo anterior, en cuanto a su ámbito de aplicación, los agentes encubiertos en línea también deben reunir las demás condiciones previstas en el artículo 12 de la ley N° 21.459, a saber: autorización judicial previa, existencia de investigación penal en curso y finalidad legítima.

El apremio de que exista una investigación en curso, se infiere de lo dispuesto en la última parte del artículo 12, inciso tercero de la ley N° 21.459, en donde se establece que, a la hora de establecer la exención de responsabilidad del agente, por los delitos que deba cometer

o que no haya podido impedir su ejecución, prevé que aquellos sean un resultado necesario del desarrollo de la investigación. También significa que las investigaciones no podrían ponerse en marcha a través de las técnicas de los agentes cibernéticos encubiertos, ni la responsabilidad penal puede basarse únicamente en el uso de esta técnica en particular, ya que debe haber otros precedentes, que no provienen de las mismas fuentes que los agentes encubiertos en línea. Los legisladores exigen explícitamente propósitos legítimos, estipulando que los agentes cibernéticos encubiertos deben tomar medidas para aclarar la conducta delictiva conforme a la ley, establecer la identidad de ciertas personas y su participación en su propia conducta delictiva, y prevenirlas o verificarlas. Por lo tanto, cualquier otro propósito del uso de esta figura con la recopilación de la prueba respectiva para un caso, quedaría fuera del alcance de la ley como medio de investigación y el efecto de eximir potencialmente al agente de responsabilidad.

Ahora bien, en violación de los requisitos del reglamento, **la falta de autorización judicial previa dará lugar a un supuesto de prueba ilegal y**, por lo tanto, no pueden utilizarse en los tribunales contra los presuntos autores de delitos informáticos involucrados, los cuales, por esa vía quedan exentos de castigo. Asimismo, la exención de responsabilidad penal de un agente debe ajustarse a lo dispuesto en la parte final del artículo 12, apartado 3. Entonces aquí los terceros que actúen bajo el influjo del agente encubierto responderán por el o los delitos que se les culpe.

Por último, decir que, se necesita tener cuidado con confundir al agente encubierto en línea con la figura del agente provocador. El primero, como se puede colegir de lo expresado, ejerce su función respecto de una realidad delictiva preexistente, la que queda en evidencia a partir de la información que este logra recabar para eventualmente utilizarla como prueba. En cambio, el agente provocador, de un modo equivalente al de un instigador, el cual crea en otros un propósito criminal, que termina en la materialización de perpetración del delito.

VI.6 Desafíos en torno a la investigación de delitos informáticos

El primer desafío a mencionar, es ver en la práctica si estas nuevas técnicas investigativas otorgadas por la ley N° 21.459 son aplicables a la realidad nuestra y si van a poder ser entendidas por los agentes que las realizan, como intervinientes en la investigación.

Es decir, por la Policía, por el Ministerio Público, por el Tribunal, cuando después se otorguen las pruebas a presencia del Tribunal.

En segundo lugar, es desafiante observar, si la ley va a ser lo suficientemente interpretable y ajustable, para ir acomodándose a la evolución que va a conllevar este tema. En el fondo, la pregunta ahora es, si esta ley va a permitir ser un paraguas que nos permita ir ajustando la investigación a toda la evolución que tiene esta materia, en donde aparecen nuevas formas delictivas todos los días.

Hay que precisar si lograremos con esta ley cubrir y dar herramientas para una investigación, que a lo largo del tiempo conlleve a obtener una correcta persecución de la delincuencia en el ciberespacio.

Al día de hoy se debe estar trabajando en las definiciones de cómo aplicar eficientemente las facultades otorgadas para investigar por parte de la ley N° 21.459, pero evidentemente hay una casi nula experiencia práctica que haya pasado por la interpretación jurisprudencial hasta este momento tomando como referencia Mayo del año 2023, la cual se va a intensificar con el tiempo y, se espera, sea para mejor análisis de este tema, para contar mayor experiencia en el ámbito de jurisprudencia y ver finalmente si se le va a dar un uso de acotado o ampliado a estas facultades, porque todavía no se está expuesto en gran medida a los tribunales de justicia.

Hasta el día de hoy, para la utilización de estas facultades, solamente se cuenta con el texto legal y la interpretación que se le puede dar al momento de dirigir las investigaciones.

En tercer lugar, cabe mencionar que hay símiles doctrinarios y jurisprudenciales en otras partes de la legislación, a modo de ejemplo, el agente encubierto online tiene un símil en la ley N° 20.000[119]. Entonces, es bueno que en la práctica se pueda ir estableciendo ya de manera notoria, el actuar de las investigaciones. Sin embargo, a nivel institucional, aún no se puede tener ya fijados criterios de actuación frente a estas nuevas herramientas, en donde se pueda decir cuáles serán exactamente los criterios a ocupar, dado que, puede ser que no los

[119] Ley 20.000. Artículo 25, párrafo 3 en adelante.

haya, como de igual forma se puede dar la opción que sean herramientas que se vayan resolviendo como caso a caso.

En relación con el obstáculo mencionado, podría ser útil revisar estas herramientas que tienen símiles a nivel nacional y también símiles a nivel internacional de cómo se han interpretado y se han ido utilizando para ver la manera de aterrizar estas facultades a nivel nacional.

En cuarto lugar, un desafío importante y de trascendencia a mentar, es que la ley no resuelve cuando el ministerio público requiere de autorización judicial para solicitar ciertos datos. Entonces, por ejemplo, durante la tramitación de la ley existían normas que apuntaban a poder distinguir si eran datos de abonado o dirección IP[120].

El ministerio público en ese caso no requeriría de autorización judicial, pero sí eran datos de tráfico o de comunicaciones, si necesita requerir autorización judicial. Eso generó un debate extenso a nivel legislativo y finalmente no se dejó una norma que pudiera resolver el conflicto. En ese caso, el desafío es súper importante para el ministerio público a nivel institucional, porque evidentemente la exigencia de autorización judicial hace mucho más difícil avanzar en una investigación de delitos informáticos propiamente tales, donde muchas veces sólo se tiene un correo, o plataforma desde donde se cometió el delito. Si el ministerio público no puede llegar al origen de la comisión del delito, la investigación se va a tornar de vasta complejidad.

En quinto lugar, está el desafío en lo que se refiere a la cooperación internacional. Relacionado a este tema cabe señalar que la mayor cantidad de proveedores no están en Chile. Debido a lo anterior, el ministerio público como organismo investigador se tiene que poner en contacto a través de procedimientos que están establecidos, a proveedores que se encuentran en otras partes del mundo, Estados Unidos, por ejemplo, con la empresa WhatsApp[121].

[120] Historia de la ley 21.459. Primer trámite constitucional Senado. Pág. 11
[121] WHATSAPP. *Información para las fuerzas del orden*. Consultado el 26 de Abril de 2023. Recuperado de: https://faq.whatsapp.com/444002211197967/?locale=es_LA.

Los países han establecido protocolos para solicitar informaciones privadas de usuarios como medio de prueba, a modo de ejemplo, se puede enunciar conversaciones entre usuarios que sean relevantes para un juicio. Estos protocolos establecidos son sumamente formales y tienen pasos que no pueden ser obviados para poder acceder a la información.

Por ejemplo, si se necesita obtener información de una cuenta en la plataforma llamada Facebook[122], se tiene que recurrir a lo que se denomina la autoridad central. Aquella que puede pedir una información a su similar en el país en el que uno está solicitando, por ejemplo, en nuestro caso corresponde a una unidad del Ministerio Público que corresponde a la Unidad de Cooperación Internacional y Extradición (UCIEX)[123]. De tal manera que si un fiscal manda un oficio o una comunicación a esta unidad, ella se entiende con su símil en el país donde está este proveedor, en este caso en el ejemplo de Facebook en Estados Unidos. Ahí se pedirá que se envíen, por ejemplo, los datos que sigan por ejemplo una IP o una cuenta que hizo tal movimiento, tal día, en tal momento, etc. Lo anterior es una parte del proceso, porque otra distinta es lograr que la empresa que está regida por la ley del país en el que está su sede, otorgue esta información al Ministerio Público.

Entonces, a futuro tenemos la incertidumbre de no saber cómo va a ir desarrollándose en gran medida la cooperación entre el Ministerio Público y los proveedores internacionales. Claramente, se van a tener nuevas herramientas que efectivamente antes no existían, para este tipo de delito, no obstante, sabemos cómo van a funcionar en la práctica. Y aun así teniendo esta mayor cantidad de herramientas, no se puede anticipar el éxito investigativo, porque hay proveedores que están fuera del control legislativo nacional. Entonces en la práctica puede acontecer que el ministerio público pueda no necesitar autorización para solicitar determinado antecedente de acuerdo a la ley chilena, sin embargo en el país donde se encuentra el proveedor si se necesita, entonces se necesita realizar algo poco ortodoxo, que es, pedir autorizaciones en Chile para que puedan ser ejecutables en otro país internacionalmente.

---

[122] FACEBOOK. *¿Puedo obtener la información o el contenido de una cuenta con una orden judicial?* Consultado el 26 de Abril de 2023. Recuperado de:

[123] FISCALÍA DE CHILE. *UCIEX*. Consultado el 1 de Abril de 2023. Recuperado de: http://www.fiscaliadechile.cl/Fiscalia/quienes/fiscaliaNac_unidades_divisiones.jsp#:~:text=Unidad%20de%20Cooperaci%C3%B3n%20Internacional%20y%20Extradiciones%20(UCIEX)&text=UCIEX%20es%20la%20Unidad%20encargada,encargados%20de%20la%20persecuci%C3%B3n%20penal.

Con la ratificación del segundo protocolo del *"Convenio de Budapest"* por parte del Congreso, se podría facilitar en gran cantidad, la cooperación internacional en estos temas.

Ahora en cuanto a la amplitud de las facultades policiales para la investigación y recaudación de prueba, evidentemente siempre hay que ponderar y tener como objetivo final la protección de las garantías constitucionales, pero también incluir en la balanza que, si no se tienen las suficientes herramientas de investigación en este tipo de delitos, es muy difícil avanzar en una correcta dirección.

En relación al delito informático, si no se puede tener ni siquiera el dato de abonado, por ejemplo, o de la dirección IP, que es algo sumamente básico e importante para el ámbito investigativo, no se tiene de donde poder desenredar la comisión del delito en un caso respectivo. Entonces sí, hay que ponderar las garantías constitucionales, pero también pensando que este es un fenómeno real de delincuencia donde hay que perseguir e investigar de forma eficaz.

Actualmente, tomando como referencia el año 2023, se están cometiendo delitos informáticos que no están siendo identificados y que no están siendo condenados. Se hace atingente un cambio en el sentido de verdad, de lo contrario nos mantendremos todavía en el plano de la teoría, y eso se vuelve un problema a enfrentar.

Cerrando este capítulo, tomando referencia lo relatado en párrafos *supra*, el proceso penal es una eterna lucha de hasta dónde se limitan garantías en todos los delitos. Cada uno, a partir de la postura que tenga, va a contestar esa pregunta. Si se es más o menos garantista o si se está de acuerdo desde una línea u otra del tema. Y desde luego, esa respuesta incide en cómo va a ser tratado este tema en la realidad. Sin embargo, ese es un punto súper importante a entender. Este no es un ejercicio de laboratorio, esto es la realidad. La gente comete delitos que afectan a otras personas y hay organismos estatales con una organización predeterminada orientados a perseguir esos delitos, otros a defender a aquellos perseguidos y un tercero imparcial a determinar si hay suficiente prueba para condenar. Entonces, si las facultades entregadas al Ministerio Público y policiales, que la nueva ley otorga son suficientes o no, va a depender de cuál es tu postura frente a la persecución, digamos, de la política pública que se quiera implementar.

VII. CONCLUSIONES

Dadas las nuevas y atingentes necesidades de hacer frente a un delito cada vez más variado y frecuente, es necesario tomar medidas serias en el asunto. Destacando que no es un ataque físico, sino “invisible”, se hace necesario encontrar soluciones e imponer barreras de seguridad, dado que se puede llegar a límites muy altos y dificultosos de manejar.

Es plausible el avance de la ley N° 19.223 a la ley N° 21.459, la cual evidentemente es el fruto de un esfuerzo por avanzar no solamente en el ámbito sustantivo, sino que también en el ámbito más procedimental e investigativo. Es una normativa que va en la dirección correcta. No obstante, en la actualidad no se puede dar mayores certezas de cómo se encuentra Chile en la actualidad en torno a la eficiencia de persecución de delitos informáticos, dado la poca utilización en la práctica de esta ley, sobre todo viéndolo desde una perspectiva investigativa. Una vez contando con mayor jurisprudencia al respecto, se podrá realizar un mayor análisis de cómo los tribunales chilenos de justicia y la doctrina reaccionará a la ley 21.459.

Sin embargo, analizando la ley se hará necesario en lo porvenir, efectuar modificaciones legales para lograr otorgar una eficiente investigación de los delitos informáticos y recopilación de pruebas, sopesando el investigar con la protección de las garantías constitucionales, incluyendo en la balanza y teniendo claridad que, de no tener las suficientes herramientas de investigación en este tipo de delitos, es muy difícil avanzar en una correcta dirección. Se debe estar conscientes de que este es un fenómeno real de delincuencia, donde hay que perseguir e investigar de forma eficaz, no sólo es legislar, sino poner en práctica de manera explícita las potestades, atribuciones y logística de persecución del delito informático.

Por otro lado, reforzar las medidas de ciberseguridad es una necesidad urgente tanto en el Ministerio Público, Poder Judicial, en los equipos de las brigadas especialistas de investigación policial de este tipo de delitos, para evitar ataques cibernéticos de criminales al sistema logrando dañarlo, como de igual forma es necesario reforzar las medidas en todos los organismos públicos que protegen la infraestructura crítica del país, no olvidándose que el sector privado debe reforzarse de similar manera, puesto que un ataque cibernético a una empresa puede afectar el patrimonio, trabajo, etc., de miles o millones de ciudadanos.

Los directorios de compañías se deben interesar en este tema, dado que hoy en día una de las amenazas más grandes al derecho de propiedad en el mundo, afecta la propiedad de los consumidores de las compañías. La recomendación, como en los manuales de gestión directiva, apunta a que en las organizaciones privadas esto se evalúe, se liste como uno de los riesgos que también existen, o sea, no únicamente los riesgos laborales o financieros.

Se hace necesario de igual forma lograr una especialización de las fuerzas policiales en torno al ciberespacio que vaya en constante actualización, respecto a las distintas plataformas digitales y sistemas operativos que hoy en día abundan y crecen cada vez con mayor fuerza.

En Chile, a nivel de sociedad, es inevitable crear una **cultura de la ciberseguridad**, que apunte a **funcionarios, trabajadores tanto del mundo privado o público**, para que estén conscientes de las cosas que hay o no que hacer en la red.

Ejercicios tan básicos como no compartir una contraseña en sitios no seguros o no guardar contraseñas en cualquier sitio web, se vuelve un trabajo imprescindible a realizar como sociedad, tanto en el ámbito público como privado. Y esta es una cuestión bien crítica en tiempos de teletrabajo, donde en múltiples ocasiones los trabajadores utilizan sus propios dispositivos para trabajar. He ahí entonces que nos encontramos frente a un tema complejo, que excede lo penal, pero imprescindible de abordar.

Para ir concluyendo y simplificando la forma de ver las cosas, es necesaria mayor capacitación y recursos es lo que pide a gritos esta materia, en esferas públicas y privadas. O sea, inversión a gran escala, logrando efectividad a modo de ejemplo desencriptar datos, valerse de las medidas específicas de investigación que están reguladas en el artículo 12 de la ley N° 21.459. Cabe recalcar que no puede pretenderse combatir el cibercrimen sin una inversión suficiente a tono de lo que exige la persecución de los delitos informáticos.

Por último, y no menos importante mencionar, de poco servirá tener un código penal despampanante, que abarque un sinfín de materias, si luego en la práctica la investigación y recopilación de prueba no se hará de buena forma, encontrando trabas en un ámbito sofisticado y técnicamente complejo como la informática.

VIII. BIBLIOGRAFÍA

1. ACURIO DEL PINO, S. (2011): *Delitos informáticos: Generalidades*. Consultado el 11 de Abril de 2023. Disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

2. ÁLVAREZ, M. (2001) *Consideraciones político criminales sobre la delincuencia informática.* Dialnet. Consultado el 10 de Septiembre de 2022. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=289088.

3. ÁLVAREZ, D. (2017). *Los desafíos de la ciberseguridad en Chile.* Revista chilena de Derecho y Tecnología. Consultado el 1 de Octubre de 2022. Recuperado de: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842017000200001.

4. ALDONEY, R. ALBERTZ, P. & ALCAÍNO E. (2022). *Nueva Ley de Delitos Informáticos: aspectos penales y de compliance.* Estudio Jurídico Carey. Consultado el 17 de Marzo de 2023. Recuperado de: https://www.carey.cl/nueva-ley-de-delitos-informaticos-aspectos-penales-y-de-compliance/.

5. ARBALÁEZ, M. (2014). *Las tecnologías de la información y la comunicación (TIC) un instrumento para la investigación*. Consultado el 4 de Febrero de 2023. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81462014000200001.

6. BANDERAS, R (2009). *¿Sociedad de la información o sociedad del conocimiento?.* El Cotidiano.

7. BARRERA, V. (2022). *Se publica Ley que moderniza normas sobre delitos informáticos.* Thomson Reuters. Consultado el 2 de Diciembre de 2022. Recuperado de: http://www.laleyaldia.cl/?p=16162.

8. BARRIOS, V. (2018). *Política Nacional de Ciberseguridad: 2017-2022*. Biblioteca del Congreso Nacional de Chile. Disponible en:

https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf.

9. BATARSE, C. (2022). *Gobierno registra 170 alertas por vulnerabilidad similares a los hackeos del Poder Judicial y las Fuerzas Armadas.* Diario La Tercera. Consultado el 10 de Diciembre de 2022. Recuperado de: armadas/TYYG46Q6KFD4LDC7IJPU63TQOE/.

10. BEJIDE. J. (2023). *Ciberataques en Chile. Una amenaza virtual, pero real.* Diario El Mostrador. Consultado el 24 de Marzo de 2023. Recuperado de: https://www.elmostrador.cl/noticias/opinion/columnas/2023/03/05/ciberataques-en-chile-una-amenaza-virtual-pero-real/.

11. BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. (2022). *Delitos Informáticos.* Consultado el 29 de Febrero de 2023. Recuperado de: https://www.bcn.cl/portal/leyfacil/recurso/delitos-informaticos.

12. BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia del Decreto Supremo Nº 83. Aprueba el Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre 2001*. Consultado el 19 de Diciembre de 2022. Recuperado de: https://www.bcn.cl/historiadelaley/historia-de-la-ley/vista-expandida/6527/#:~:text=El%20Convenio%20sobre%20la%20Ciberdelincuencia%20del%20Consejo%20de%20Europa%2C%20conocido,y%20de%20otros%20sistemas%20inform%C3%A1ticos.

13. CAVADA, J. (2015). *Delitos Informáticos. Chile y legislación extranjera*. Biblioteca del Congreso Nacional. Disponible en: Https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/22170/3/Delitos%20Inform%C3%A1ticos%202015.pdf.

14. CAVADA, J. (2020). Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera. Biblioteca del Congreso Nacional. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf.

15. CARRASCOSA, V. (1995). *"El Derecho Informático como asignatura para juristas e informáticos"*. Revista de Informática y Derecho, Universidad Nacional de Educación a Distancia. Merida.

16. CIBERSEGURIDAD. *Ciberespacio.* Consultado el 6 de Enero de 2023. Recuperado de: https://ciberseguridad.com/guias/recursos/ciberespacio/.

17. CÓDIGO CIVIL DE CHILE.

18. CÓDIGO PENAL DE CHILE.

19. CÓDIGO PROCESAL PENAL DE CHILE.

20. CÓDIGO PENAL ESPAÑOL.

21. CONVENIO SOBRE LA CIBERDELINCUENCIA.

22. CÓRDOBA, J y GARCÍA, M. (2004) *Comentarios al Código Penal*, *parte especial*. Tomo I. Madrid-Barcelona. Aranzadi.

23. CSIRT. *Hitos de la historia de Internet.* Consultado el 4 de Abril de 2023. Recuperado de: https://www.csirt.gob.cl/noticias/hitos-de-la-historia-de-internet/.
24. CSIRT. *Quiénes somos*. Consultado el 17 de Agosto de 2022. Recuperado de: https://www.csirt.gob.cl/quienes-somos/.

25. MINISTERIO DE RELACIONES EXTERIORES . *Decreto 83.* Diario Oficial de la República de Chile. Santiago, Chile, 28 de Agosto de 2017.

26. DONOSO ABARCA, L. REUSSER MONSÁLVEZ, C.(2021). *Derecho Informatico*. Academia Judicial.

27. EQUIPO CEEAG. (2016). *Desafío para afrontar la ciberguerra.* Tema De Investigación Central De La Academia. Disponible en: https://publicacionesacague.cl/index.php/tica/article/view/180.

28. ESPINOZA CORREA, C. (2014). *Delitos Informáticos y la Ley 19.223.* Revista Actualidad Jurídica.

29. FISCALÍA DE CHILE. *UCIEX*. Consultado el 1 de Abril de 2023. Recuperado de: http://www.fiscaliadechile.cl/Fiscalia/quienes/fiscaliaNac_unidades_divisiones.jsp#:~:text=Unidad%20de%20Cooperaci%C3%B3n%20Internacional%20y%20Extradiciones%20(UCIEX)&text=UCIEX%20es%20la%20Unidad%20encargada,encargados%20de%20la%20persecuci%C3%B3n%20penal.

30. GARCÍA, J. (2008) *El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico*. Disponible en: https://revistas.comillas.edu/index.php/revistaicade/article/download/357/283.

31. GLOBAL CYBER SECURITY CAPACITY CENTRE UNIVERSITY OF OXFORD. (2016). *Modelo de Madurez de Capacidades de Ciberseguridad para Naciones* (CNM). Disponible en: https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7840

32. GONZÁLEZ, C. (2022). *Alerta por ataque informático al Poder Judicial: Jueces deben realizar audiencias desde celulares y no abrir correos dudosos.* Diario El Mercurio On-Line. Consultado el 28 de Ocubre de 2022. Recuperado de: https://www.emol.com/noticias/Nacional/2022/09/26/1073829/ataque-informatico-al-poder-judicial.html.

33. HERNÁNDEZ, C. (1999). *Hackers, Los Piratas del Chip y de Internet.* Libro electrónico gratuito. Disponible en: http://.perso.wanadoo.es/snickers.

34. Historia de la ley 21.459, Primer trámite constitucional Senado.

35. HORVITZ, M. & LÓPEZ, J. (2003) *Derecho Procesal Penal Chileno*. Tomo I. Santiago: Editorial Jurídica de Chile.

36. HORVITZ, M. y LÓPEZ, J. (2017). *Derecho Procesal Penal Chileno*, *Tomo I*, reimpresión de la 1a ed. Santiago: Editorial Jurídica de Chile.

37. HORZELLA, B. (2021). *Política nacional de Ciberdefensa.* Biblioteca del Congreso Nacional de Chile. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe_BCN__Politica_Nacional_de_Ciberdefensa.pdf

38. JIJENA LEIVA, R. (2012). *La criminalidad informática: situación de lege data y lege ferenda en CHILE.* Informática y Derecho.

39. KASPERSKI. *¿Qué es la ciberseguridad?.* Consultado el 18 de Octubre de 2022. Recuperado de: center/definitions/what-is-cyber-security.

40. LAGOS, F. (2022). (Comentario en la página Web). Twitter. Consultado el 2 de Noviembre de 2022. Recuperado de:https://twitter.com/Zerial/status/1574401080385048577?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1574401080385048577%7Ctwgr%5Ee3f4fa541f46859110767a749411011f44879c5e%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.biobiochile.cl%2Fnoticias%2Fciencia-y-tecnologia%2Fpc-e-internet%2F2022%2F09%2F30%2Fciberataques-a-entidades-gubernamentales-por-que-ocurren-y-que-se-puede-hacer-para-evitarlos.html.

41. Lara, J. C., Martínez, M., & Viollier, P. (2014). *Hacia una regulación de los delitos informáticos basa-da en la evidencia.* Revista Chilena De Derecho Y Tecnología, 3(1). Pág 105. Disponible en: https://doi.org/10.5354/0719-2584.2014.32222.

42. LEY 18.168.

43. LEY 20.000.

44. Ley 20.393

45. LEY 21.459.

46. LIBICKY M. (2000). *The future of information Security*, Institute for National Strategic Studies.

47. LÓPEZ DE ARENOSA, R. (1994). *IRIS, red informática del Plan Nacional de I + D*. Política Científica, n° 40, julio.

48. MAYER LUX, L. (2018) *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos.* Scielo. Consultado el 4 de Noviembre de 2022. Recuperado de https://www.scielo.cl/scielo.php?pid=S0718-00122018000100159&script=sci_arttext#:~:text=La%20criminalidad%20inform%C3%A1tica%20se%20caracteriza,%E2%80%9Cglobalizaci%C3%B3n%20del%20delito%E2%80%9D57.

49. MAYER LUX, L., & OLIVER CALVERÓN, G. (2020). *El delito de fraude informático: concepto y delimitación.* Revista Chilena De Derecho Y Tecnología. https://doi.org/10.5354/0719-2584.2020.57149.

50. MAYER LUX, L. & VERA, J. (2020). *El delito de espionaje informático: Concepto y delimitación.* Scielo. Consultado el 22 de Marzo de 2023. Recuperado de: ttps://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071925842020000200-221.

51. MAYER LUX, L. & VERA, J. (2020). *La falsificación informática:. ¿Un delito necesario?.* Scielo. Consultado el 21 de Marzo de 2023. Recuperado de: https://www.scielo.cl/scielo.php?pid=S071925842022000100261&script=sci_arttext.

52. MAYER LUX, L & VERA, J. (2022). *La nueva ley de delitos informáticos. Vol. XLVIII. N°3.* Revista de Ciencias Penales. Pág. 321. Disponible en: http://revistadecienciaspenales.cl/wp-content/uploads/2023/04/RCP-3-2022-Final-273-342.pdf.

53. MICROSOFT. *Definición de los ataques DDOS.* Consultado el 12 de Marzo de 2023. Recuperado de: https://www.microsoft.com/es-ar/security/business/security-101/what-is-a-ddos-attack.

54. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. *Sociedad de la Información.* Consultado el 19 de Diciembre de 2022. Recuperado de: https://mintic.gov.co/portal/inicio/Glosario/S/5305:Sociedad-de-la-Informacion.

55. MINISTERIO DE INTERIOR Y SEGURIDAD PÚBLICA (2017). *Política Nacional de Ciberseguridad.* Disponible en: https://digital.gob.cl/biblioteca/estrategias/politica-nacional-de-ciberseguridad-2017-2022/.
56. MIRÓ LLINARES. F (2012). *El Cibercrimen*. Marcial Pons. Madrid.

57. NAVEDA, J. (2021). C*hile es el país con mayor proporción de conexiones a internet de Latinoamérica.* Comscore. Consultado el 2 de Noviembre de 2022. Recuperado de: https://www.comscore.com/lat/Prensa-y-Eventos/Blog/Chile-es-el-pais-con-mayor-proporcion-de-conexiones-a-Internet-de-Latinoamerica#:~:text=Chile%20es%20el%20pa%C3%ADs%20latinoamericano,76%25%20de%20la%20poblaci%C3%B3n%20total.

58. OLIVETTI, C. (2019). *¿Qué es la Ciberética?.* (Comentario en la página web*).* Linkedin. Consultado el 3 de Septiembre de 2022. Recuperado de: https://es.linkedin.com/pulse/qu%C3%A9-es-ciber%C3%A9tica-carmen-olivetti.

59. PÉREZ-LUÑO, A. (1996), *Manual de informática y derecho*, Editorial Ariel, Barcelona.

60. PICOTTI, L. (1989). *“La criminalità...”*, cit.

61. PODER JUDICIAL REPÚBLICA DE CHILE. (2022). *Poder Judicial presenta denuncia criminal por incidente de ciberseguridad*. Consultado el 10 de Diciembre de 2022*.* Recuperado de: https://www.pjud.cl/prensa-y-comunicaciones/noticias-del-poder-judicial/79577.

62. PORTALES, M. (2022). *Nuevo Catálogo de Delitos Informáticos y Compliance Penal.* Círculo Inhouse. Consultado el 29 de Noviembre de 2022. Recuperado de: https://circuloinhouse.cl/compliance/nuevo-catalogo-de-delitos-informaticos-y-compliance-penal/.

63. PRANDINI, P. MAGGIORE, M. (2013). *Ciberdelito en América Latina y el Caribe. Una visión desde la sociedad civil.* Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe.

64. PROYECTO DE LEY 14.847-06. (2022). *Establece una Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información.* Ingreso de Proyecto. Pág. 6. Consultado el 30 de Abril de 2023. Disponible en; https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15344&prmBOLETIN=14847-06.

65. REAL ACADEMIA ESPAÑOLA. *Red Social.* https://dpej.rae.es/lema/red-social.

66. REYES ECHANDÍA, A, *La Tipicidad*, Universidad de Externado de Colombia, 1981.

67. RODRÍGUEZ, L.(coord.) y otros.(2005) *Código Penal*. Madrid: La Ley.

68. SEPÚLVEDA, N. (2022). *Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa.* Ciper. https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/

69. UNODC. (2010). *Informe Mundial de UNODC sobre trata de personas: las crisis cambian los patrones de la trata de personas y dificultan la identificación de las víctimas.* Oficina de las Naciones Unidas contra la Droga y el Delito en México. Recuperado de: https://www.unodc.org/lpomex/es/noticias/enero-2023/informe-mundial-de-unodc-sobre-trata-de-personas_-las-crisis-cambian-los-patrones-de-la-trata-de-personas-y-dificultan-la-identificacin-de-las-vctimas.html.

70. VERDÚ, V. (1994). *Está usted entrando en Internet*. El País Semanal, año XIX, n° 198.

71. WHATSAPP. *Información para las fuerzas del orden*. Consultado el 26 de Abril de 2023. Recuperado de: https://faq.whatsapp.com/444002211197967/?locale=es_LA.

72. WINTER ETCHEVERRY, J. (2013). *Elementos típicos del artículo 2° de la Ley Nº 19.223: Comentario a la SCS de 03.07.2013 Rol Nº 9238-12.* Revista de Ciencias Penales. Disponible en: http://revistadecienciaspenales.cl/wp-content/uploads/2019/02/Corte-Suprema-6.