Universidad de Chile

Facultad de Derecho

Departamento de Derecho Procesal

Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional.

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

Alumnos: Ignacio Novoa Toledo; Leonor Venegas Cruz.

Profesor Guía: Lorena Donoso Abarca.

Santiago de Chile

julio, 2020

AGRADECIMIENTOS

Mis más sinceros agradecimientos a cada una de las mujeres que han forjado mi camino profesional y como persona, en especial a mi madre que ha forjado en mí el temple y la resiliencia, a cada uno de mis amigos y compañeros por su apoyo; a mi padre por la paciencia, y a Sayen por el amor y paz que me da.

L.V.C.

Agradezco a mis padres por su infinito cariño, por el permanente cuidado en mi formación y por las lecciones más valiosas que en mi vida siguen dando. Agradezco a toda persona que en mayor o menor medida formó parte de este intrincado camino.

I. N. T.

INDICE

RESUMEN

El 23 de noviembre de 2001, en la ciudad de Budapest se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa y otros estados invitados. El objetivo del Convenio es establecer una legislación penal y procedimientos comunes entre los suscriptores, para la persecución de delitos cometidos a través de medios electrónicos e informáticos; y a su vez, fortalecer la cooperación internacional, teniendo en cuenta el carácter transfronterizo de la información que se maneja en la red y los delitos que se cometen utilizándola como medio. El objetivo principal de este trabajo es analizar; a través del estudio y recopilación de fuentes nacionales e internacionales, la adopción de un convenio a nivel global en esta materia, cómo sus normas operan en las investigaciones de estos delitos, y cómo incorporarlas a la legislación nacional respetando el principio de proporcionalidad y la protección de los derechos fundamentales; para ello (i) se presenta el Convenio, sus antecedentes y herramientas, la asistencia jurídica internacional y el rol de los proveedores de servicio; (ii) se estudia la normativa nacional de ciberdelincuencia y la adopción del Convenio en Chile mediante su ratificación y tramitación del proyecto de adecuación; (iii) se analizan las medidas intrusivas pertinentes a ciberdelincuencia en nuestra legislación; y (iv) Damos noticia de algunos ejemplos de derecho comparado sobre la incorporación del Convenio a distintos sistemas legislativos para obtener las conclusiones finales.

INTRODUCCIÓN.

La masificación del Internet ("la Red") marcó un antes y un después en la forma de vida de las personas alrededor del mundo. De acuerdo a una encuesta realizada en 2017 por la Subsecretaría de Telecomunicaciones (SubTel)[1] a esa época un 87,4% de los hogares en Chile tenía acceso a internet, ya sea por medio de red fija o inalámbrica. A su vez, el *Global Digital 2019 reports*[2], mostró que en regiones como Norteamérica y Europa del Norte la masificación de internet en la población alcanza el 95%. Los usuarios van desde menores de 3 años hasta personas de la tercera edad. La forma de acceder a la información, de comunicarnos, de cómo trabajamos, estudiamos o compramos han sido revolucionadas por la aparición de la Red. En la actualidad, la utilización de aplicaciones para móviles permite compartir archivos e incluso nuestra ubicación de manera instantánea. Sin embargo, la apertura del ciberespacio[3] no solo ha traído beneficios y progreso en la comunidad, sino que también ha sido una herramienta para generar nuevas formas delictivas antes desconocidas tales como el *Malware*[4], *Ransomware*[5], *Pharming*[6], entre otros. Asimismo, ha permitido la comisión de delitos clásicos como la suplantación de identidad, el fraude y acoso, a través de la red, logrando un mayor alcance y extensión a la vez que el medio dificulta su persecución.

[1]BRÚJULA. IX Encuesta de Acceso y Usos de Internet - Informe Final – diciembre 2017. [en línea]: <https://www.subtel.gob.cl/wp-content/uploads/2018/07/Informe_Final_IX_Encuesta_Acceso_y_Usos_Internet_2017.pdf> [consulta: 01 de junio 2020]

[2] DIGITAL 2019. Essential insights into how people around the world use the internet, mobile devices, social media and e-commerce. 31 de enero de 2019. [en línea] <https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates> [consulta: 01 de junio 2020]

[3] El ciberespacio se ha definido como un espacio virtual de interacción que surge directamente como un lugar relacional, es decir su existencia solo será efectiva cuando haya intercambio de información, siendo por tanto espacio y medio. (AGUIRRE Romero, Joaquín. Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. Biblioteca virtual universal, Universidad Complutense de Madrid. Pág. 1. [en línea] <https://www.biblioteca.org.ar/libros/150717.pdf> [consulta: 01 de junio de 2020]

[4] Es un "software malicioso" que se inserta en los sistemas operativos o discos duros de computadores y smartphones para recolectar la información que genera el usuario. Por lo general su descarga es automática y sin previo conocimiento del usuario como archivo adjunto desde emails publicitarios falsos, páginas web, o aplicaciones.

[5] Este ciberdelito hizo su debut mundial en 2017 con "*Wannacry*", programa informático malintencionado que impidió el acceso a la información de determinados archivos o todo el disco duro de computadores de empresas en todo el mundo. Su valor está en que cifra los datos para hacerlos imposibles de acceder excepto por un sistema de descifrado específico que los *hackers* desarrollan para ese fin, previo pago de una cuantiosa suma de dinero o *bitcoins*.

[6] Es la explotación de una vulnerabilidad en el *software* de los servidores que permite al atacante redirigir un nombre de dominio a otra computadora distinta, de esta forma cuando el usuario ingrese un nombre de dominio será redirigido al que el atacante haya especificado.

El avance y desarrollo de las Tecnologías de Información y Comunicación (TICs) constituyen un desafío para el mundo del Derecho. El ciberespacio, la ausencia de fronteras y controles; tanto en su contenido como en su acceso, generan conflictos a nivel jurisdiccional donde los límites de los Estados no resultan eficaces. La relatividad del tiempo y espacio en la Red plantea un serio desafío para las legislaciones penales y procesales cuyo diseño y estructura se planteó siempre para combatir y sancionar una delincuencia física, donde los delitos típicos como el hurto, robo, violación, homicidio requieren de un contacto o cercanía entre la víctima y el delincuente, algo que no ocurre en la ciberdelincuencia. Es por esto que se hace necesario reformular los ordenamientos jurídico-procesales frente al avance de la ciberdelincuencia, sin renunciar a los principios básicos del derecho penal ni a los derechos fundamentales de los ciudadanos.

La ciberdelincuencia es una "industria" multimillonaria cuyas víctimas son individuos, instituciones financieras, titulares de propiedad intelectual, gobiernos, entre otras estructuras de carácter estratégico. Una de sus principales características es su alcance transnacional, que la Oficina de las Naciones Unidas contra la Droga y el Delito describe como "*un negocio ilícito que trasciende las fronteras culturales, sociales, lingüísticas y geográficas y que no conoce fronteras ni reglas*"[7]; esto tiene como consecuencia directa que los órganos encargados de la persecución de estos delitos vean restringidas sus investigaciones por las fronteras nacionales, lo que sumado al anonimato que facilita la Red, impide una persecución exhaustiva. El problema se acrecienta cuando entre Estados involucrados existen sistemas jurídicos distintos, por ejemplo en un delito cuyos efectos se presenta en un país como Chile, con un sistema continental, y cuyo origen o comisión proviene de un país del *common law* como Estados Unidos, en el que además de las leyes (*statutes*), existen normas jurídicas que emanan del derecho consuetudinario interpretado por los jueces con efectos generales (*case law*). La diferencia se acentúa si revisamos la institucionalidad de ambos países; mientras en Chile el

[7]OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO. Delincuencia organizada transnacional - La economía ilegal mundializada [en línea] <https://www.unodc.org/documents/toc/factsheets/TOC12_fs_general_ES_HIRES.pdf> [consulta: 1 de junio de 2020]

Ministerio Público es un organismo autónomo, jerarquizado[8], descentralizado e independiente el Poder Judicial, encargado de la investigación de los delitos ocurridos dentro del territorio de la República; en Estados Unidos el Departamento de Justicia de los Estados Unidos (DOJ), está directamente vinculado al gobierno de turno del país, siendo facultad del Presidente de la República establecer los criterios y formas de actuación, por lo que las políticas criminales dependerán de la agenda del gobierno central[9].

Como una forma de evitar que estas diferencias impidan la correcta y oportuna investigación de los delitos, nace la necesidad de unificar criterios normativos para abordar la ciberdelincuencia y uso de TICs, desde el punto de vista del Derecho Internacional, debiendo recurrir a la adopción de instrumentos jurídicos que se adecuen a los distintos sistemas jurídicos internacionales, a las institucionalidades, que además mantengan el respeto por los derechos humanos a través de la coordinación de redes de trabajo para la persecución efectiva, tanto a nivel regional como mundial.

El **objetivo general** de este trabajo es analizar la respuesta normativa sobre el fenómeno de la ciberdelincuencia y su acelerado avance internacional, mediante principalmente el estudio del Convenio de Budapest sobre ciberdelincuencia y su adaptación en Chile con especial atención a la proporcionalidad de las medidas.

Evaluar la importancia de contar con un marco regulatorio común en materia de ciberdelincuencia, a través del análisis del Convenio de Budapest y su estructura.

Diagnosticar la regulación nacional sobre ciberdelincuencia con especial foco en las medidas procesales.

Los **objetivos específicos** son analizar la estructura del Convenio de Budapest; qué herramientas se estiman esenciales para esta respuesta procesal penal contra la

[8] Según lo dispuesto por el artículo 83 de la Constitución Política de Chile.
[9] Estados Unidos además es un país federal, por lo cual, tiene políticas y normas internas según cada Estado, lo cual hace más compleja la cooperación y coordinación sin normas que unifiquen los criterios.

ciberdelincuencia y sus características; la realidad jurídica de nuestro país en esta materia con especial foco en las medidas procesales; cómo se implementa la normativa del Convenio en nuestro país; además de realizar un breve estudio de derecho comparado que permita obtener un mayor marco de análisis mediante el estudio de la ciberdelincuencia y su combate tanto respecto del proceso de adaptación del Convenio.

De esta manera el Capítulo I, analizará los antecedentes que llevaron a la regulación, no solo de delitos cometidos a través de medios digitales, sino además de herramientas de obtención y conservación de datos informáticos para su incorporación a los procesos judiciales, el Protocolo adicional N°189 sobre criminalización de actos de índole racista y xenófobos y el estudio sobre las herramientas de cooperación internacional contempladas en él, lo que lo convirtió en uno de los pioneros en regular estas materias a nivel macro; en el Capítulo II, revisaremos la adopción del Convenio por nuestro país, la discusión legislativa al respecto, adecuaciones a la realidad nacional y a nuestro sistema procesal penal; además se analizará el rol de las policías y el Ministerio Público para llevar a cabo las diligencias que se den en las investigaciones por los delitos que involucren medios o evidencias digitales y su incorporación en juicio. El Capítulo III de la investigación analiza el tratamiento que reciben las medidas intrusivas en general y la conservación de datos y el agente encubierto en particular en distintas leyes nacionales, y como se ven complementadas por el Convenio; finalmente, el Capítulo IV realiza un estudio sobre la adopción y adecuación del Convenio en el derecho comparado, lo que nos permite visualizar el camino que diversos Estados toman para implementar el Convenio de Budapest en su regulación local.

CAPÍTULO I.- ANTECEDENTES DEL CONVENIO DE BUDAPEST Y SU PROTOCOLO

1.- Antecedentes del Convenio, la necesidad de regular la Ciberdelincuencia y los datos informáticos como medio de prueba

La regulación jurídica de la ciberdelincuencia ha atravesado distintas etapas; a partir de los años 80, tanto en Europa como en Estados Unidos surgen las primeras normas jurídicas que regulan y penalizan delitos cometidos mediante el uso de internet; sin embargo el concepto de ciberdelincuencia era muy restringido; así, en el año 1984, en Estados Unidos se dictó la Ley de Fraude y Abuso Informático (CFAA, por sus siglas en inglés)[10], respecto de aquellos casos de fraude, acceso ilegal y vandalismo informático. Esta normativa tipificó siete conductas relativas a acceso ilegal a computadoras; sin embargo, esta norma solo hacía referencia a "ordenadores protegidos", es decir, aquellos utilizados por instituciones financieras, gobierno federal, o usados en comercio o comunicaciones con terceros Estados. Ya en los años 90 tanto Europa como América contaban con normativa sobre cibercrímenes cometidos dentro de sus propios países. Esta legislación interna, asumía que las actividades delictivas ocurrirían por completo dentro de las fronteras territoriales de la nación, y que tanto ofensor como víctima, si no eran ciudadanos de la misma nación, estaban a lo menos situados al interior de ella cuando estos ilícitos acaecían[11].

Las implicancias económicas que podría traer el abuso de internet y su uso indebido poniendo en peligro la seguridad de transacciones económicas, que comenzaban a masificarse a través de la Red; el mal uso de la información almacenada en las bases de datos de instituciones públicas, o privadas, llevaron a que en el año 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) identificara sus análisis y acciones sobre este problema e

[10] ESTADOS UNIDOS. 18 US Code. § 1.030. [en línea] < http://bcn.cl/1nmu1> [consulta: 1 de junio de 2020]

[11] Esta suposición tiene sustento histórico para la actividad criminal. *"El comercio a lo largo del tiempo comenzó a trascender las fronteras y legislaciones nacionales, en cambio la criminalidad mantuvo un carácter provincial en su mayor parte, porque ésta supone una dinámica personal, un cara a cara entre la víctima y el ofensor. Así, por ejemplo, es imposible incurrir en el delito de violación si el violador y la víctima están a cinco millas de distancia; y, en un entorno no tecnológico, es igualmente imposible hurgar en los bolsillos de alguien o tomar su propiedad por la fuerza si el ladrón y la víctima están en diferentes países."* (BRENNER, Susan. La Convención sobre Cibercrimen del Consejo de Europa - Revista Chilena De Derecho Y Tecnología Centro De Estudios En Derecho Informático. Universidad De Chile -ISSN 0719-2576. Vol. 1 Nro. 1 (2012). 224 p.)

implementara estudios con el fin de armonizar a nivel internacional las normas que sancionaban y regulaban materias informáticas. Dicho trabajo culminó en 1986 con la emisión del reporte titulado "Delitos de Informática", en el cual se recomendaba la penalización de un listado de conductas calificadas como ciberdelitos. En paralelo, el Comité europeo para los problemas criminales (CDPC)[12] del Consejo de Europa estableció un grupo especializado de expertos en materia de delitos informáticos, el cual recogió la información obtenida en los reportes de la OCDE, y que con el paso de los años fueron ampliando el catálogo de delitos a temáticas como la protección de la privacidad, protección a la víctima, prevención, asuntos procesales como la investigación, confiscación internacional de datos y la cooperación internacional durante la investigación[13]. El trabajo del CDPC concluyó con la Recomendación (89)9, la cual sugería la revisión de las directrices para legisladores en materias de "*delincuencia relacionada con computadoras"*[14]. Dentro de los informes emitidos se remarcaba la necesidad de mantener actualizada la regulación penal conforme los desarrollos tecnológicos; y, por otra parte, la urgencia de realizar un trabajo internacional conjunto para combatir la delincuencia transnacional de carácter cibernética[15].

A raíz de la Decisión del CDPC, en la 583va reunión de Ministros del Consejo de Europa se estableció el nuevo comité denominado "Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY)" el cual comenzó su labor en el año 1997 sobre el proyecto de un convenio internacional contra la ciberdelincuencia.

[12] El CDPC o Comité Europeo de Problemas de Crimen, tiene por objetivos 1. Supervisar y coordinar las actividades del Consejo de Europa en el campo de la prevención y el control del delito. 2. Identificar las prioridades para la cooperación legal intergubernamental, hacer propuestas al Comité de Ministros sobre actividades en los campos de derecho penal y procesal, criminología, e implementa estas actividades. 3. Elaborar convenciones, recomendaciones e informes. Organizar conferencias de investigación y coloquios criminológicos, conferencias de directores de administración penitenciaria. <https://www.coe.int/en/web/cdpc> [consulta: 1 de junio de 2020]

[13] ESTRADA, Rodolfo y Somellera, Roberto. *Delitos informáticos*. Instituto Tecnológico y de Estudios Superiores de Monterrey. Campus Estados de Niéxú·o Dialnet. 436 p.

[14] Íbid.

[15] *"el derecho penal debe mantenerse al corriente de estos desarrollos tecnológicos que ofrecen oportunidades muy sofisticadas para hacer un mal uso de las facilidades del ciberespacio y perjudicar intereses legítimos. Dada la naturaleza transfronteriza de las redes de información, es necesario un esfuerzo internacional concertado para hacer frente a ese uso impropio."* CONSEJO DE EUROPA. Informe explicativo Convenio de Budapest. 3 p. <https://rm.coe.int/16802fa403> [consulta: 1 de junio de 2020].

Con arreglo a la decisión tomada por el Comité PC-CY, una primera versión del proyecto fue desclasificada y publicada en abril de 2000, la que fue seguida de versiones posteriores publicadas al término de cada reunión plenaria con el fin de que los Estados negociadores pudieran efectuar consultas con todas las partes interesadas. El proyecto del Convenio revisado y finalizado, así como su Memorando Explicativo fueron sometidos a aprobación del CDPC en junio de 2001, después de lo cual el texto del proyecto de Convenio fue sometido al Comité de Ministros para su aprobación, quedando abierto para su firma el 23 de noviembre de 2001, en la ciudad de Budapest, Hungría.

La acogida que ha tenido el Convenio a nivel internacional ha sido positiva, en general, sin embargo, algunos Estados han preferido no adherir al Convenio, ya que estiman que la forma en que se debe regular tanto la cooperación internacional, como las materias de ciberdelincuencia debería darse mediante tratados regionales que contemplen la forma de trabajo y necesidades de la región. En este sentido, el alcance y desarrollo de la ciberdelincuencia en América Latina es menor en comparación a algunos países de Asia o Europa[16]. En la misma línea países como Brasil e India se han restado de adoptar el Convenio sobre la base de que no participaron en su redacción; los países del grupo BRIC[17] y afines argumentan que por motivos técnicos y políticos el Convenio de Budapest no es una respuesta suficiente al problema y buscan un mandato para la elaboración de un instrumento jurídico universal bajo el auspicio de las Naciones Unidas.[18] En la misma línea se encuentra la Organización de Cooperación de Shanghái (OCS) que además de los países euroasiáticos de BRICS agrupa a: Kazajistán, Kirguistán, Tayikistán, Uzbekistán y Pakistán. Todos ellos, con excepción de Brasil, poseen una visión del ciberespacio profundamente ligada a la soberanía,

[16] "*Estados Unidos y Rusia se sitúan notablemente por encima del resto de países, participando con un 37,8% y un 12,3% respectivamente como origen de estos ataques. Añadiendo además que ambos países suponen igualmente los mayores contribuyentes a la creación de software malicioso participando con un 39,4% de las creaciones de malware por parte de Estados Unidos y un 19,7% por parte de Rusia*". MATEOS Pascual, Iván. 2013. Ciberdelincuencia, desarrollo y persecución tecnológica. Universidad politécnica Madrid. Sophos Security Threat Report. 109 p. [En línea] <http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf> [consulta: 01 de junio 2020]

[17] El grupo BRIC, actualmente BRICS, es la sigla para denominar al grupo de países compuesto por Brasil, Rusia, India, China y Sudáfrica, que forman una asociación económica comercial de los países cuyas economías son las más emergentes del mundo.

[18] GILLES Bélanger, Pierre. Derechos Humanos Y El Derecho Penal En El Ciberespacio. Revista secretaria tribunal permanente de revisión Año 5, N.º 10; octubre 2017; Centro de Derechos Humanos de la Universidad de Ottawa, Canadá. 280 p.

que se contrapone al modelo europeo y la hace incompatible con los mecanismos que propone el Convenio.[19]

2.- Estructura del Convenio.

El 23 de noviembre de 2001, en la ciudad de Budapest se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa[20], como también para aquellos países que, sin formar parte de este, quisieran adoptar la normativa contenida en él. El Convenio, viene a complementar otros tratados existentes en el Consejo de Europa en materia de cooperación en materia penal[21], pero manteniendo el foco en dos objetivos principales; en primer lugar, mejorar la eficacia de las investigaciones y procedimientos penales relativos a delitos cometidos a través de la Red, y, por otra parte, permitir la obtención y mantención de la evidencia electrónica obtenida en estas investigaciones, con miras a su inclusión en juicio.

En esencia, el Convenio requiere que los Estados Parte ajusten su normativa interna, de manera que sean conformes con las disposiciones que implementa; de esta forma, requiere, por una parte, incluir los tipos penales enlistados y definidos por el mismo Convenio; y, por otra, dotar a las autoridades que intervienen en la persecución penal, de las facultades y herramientas procedimentales necesarias para investigar la comisión de estos delitos, incluyendo la expansión de capacidades de inteligencia, vigilancia y herramientas; tales como, incautación de bienes, monitoreo de contenido en línea, retención y transferencia de datos e intervención de comunicaciones privadas. Respecto estas medidas y conforme al ámbito de aplicación establecido por el propio Convenio[22], dichas instituciones no estarán restringidas a

[19] GUERRERO Argote, Carlos. De Budapest al Perú: Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia. Impacto en el corto, mediano y largo plazo. Derecho digitales América Latina. Junio 2018. 5 p.
[20] CONSEJO DE EUROPA. Listado de países miembros y observadores. [en línea] <https://www.coe.int/es/web/about-us/our-member-states> [consulta: 1 de junio de 2020]
[21]CONSEJO DE EUROPA. Complete list of the Council of Europe's treaties. [En línea] <https://www.coe.int/en/web/conventions/full-list> [consulta: 1 de junio de 2020]
[22] Artículo 22.

investigaciones por cibercrímenes, sino que serán extensivas a todos aquellos procedimientos en que existan evidencias contenida en TICs, sin importar la naturaleza del delito mismo.

En cuanto a su estructura, el Convenio de Budapest se divide en cuatro capítulos y un preámbulo, el cual se enfoca en los objetivos del Convenio, y la necesidad de armonizar a nivel internacional la persecución contra el cibercrimen. Además, en la ciudad de Estrasburgo, el 28 de enero de 2003, se aprobó el Protocolo Adicional *APCoC N° 189* que regula materias de racismo y xenofobia que se expresan por medios informáticos.

- **Capítulo I, titulado "Terminología",** contiene solo un artículo, el cual introduce algunas definiciones a efectos de comprender los conceptos utilizados en el cuerpo del Convenio[23].

- **Capítulo II, titulado "Medidas que deben adoptarse a nivel nacional**", compuesto de 3 secciones, referidas a Derecho Penal, Derecho Procesal y Jurisdicción respectivamente, en las cuales se incorporan las medidas que se deberán adoptar por cada Estado, para la entrada en vigencia del Convenio; considerando particularmente la obtención, conservación y presentación de datos informáticos dentro del procedimiento, y sus normas de jurisdicción.

- **Capítulo III, titulado "Cooperación internacional",** el que incluye normas especiales respecto el procedimiento de extradición, la asistencia mutua, la utilización y restricción de uso a la información obtenida; medidas provisionales, asistencia entre órganos de investigación, la creación de una red 24/7, entre otras.

- **Capítulo IV, titulado "Cláusulas finales",** contiene las formalidades para la firma, entrada en vigor, adhesión, reservas, solución de controversias y la denuncia del tratado, entre otros.

[23] "Sistema informático", "datos informáticos", "proveedor de servicios" y "datos relativos al tráfico".

En cuanto a la inclusión de tipos penales, el Convenio establece 4 categorías:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos,
- Delitos informáticos,
- Delitos relacionados con el contenido, y
- Delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.

Los delitos, se encuentran desarrollados entre los artículos 2 y 10 del Convenio. A la fecha de su dictación, en el año 2001, buscaban sancionar conductas que afectaban la integridad informática, tanto de personas naturales como jurídicas, castigar expresamente la difusión de material pornográfico infantil y las infracciones a las normas de propiedad intelectual[24].

En lo particular, la repercusión que tiene para Chile, la inclusión de estos tipos penales, es que, en palabras de la abogada de la Unidad Especializada en Lavado de Dinero, Delitos Económicos, Medioambientales y Crimen Organizado, de la Fiscalía Nacional, Camila Bosch, *"supone una ampliación sustancial de las normas de sanción actualmente vigentes en nuestro país en lo que respecta a ciberdelitos, teniendo en cuenta que la Ley 19.223 -que tipifica delitos informáticos- se compone únicamente de cuatro artículos en que se tipifican dos delitos, el espionaje y el de sabotaje informático".*[25] Sin embargo, y como ya mencionamos, la redacción del Convenio y sus normas permite que a posteriori estas sean aplicables a delitos que no están hoy regulados y por tanto que vaya de acuerdo con los avances legislativos y tecnológicos.

[24] Recordemos que a principios de los años 2000 se destaparon muchas redes internacionales dedicadas a la difusión de material pornográfico infantil, casos que llegaron a Chile, incluso el caso Spiniak. Además del explosivo aumento de "piratería" a obras musicales y cinematográficas disponibles al público.

[25] BOSCH, Camila. Evidencia digital. 2018 El Convenio de Budapest y sus desafíos en el Derecho Procesal Penal. Revista Jurídica Ministerio Público. ISSN: 0718-6479. N°72. 123 p.

Tanto la regulación en materia procesal, como de cooperación internacional, serán analizadas posteriormente de manera particular, en los títulos III y IV respectivamente.

3.- Herramientas contempladas en el Convenio.

En materia procesal, el Convenio prevé normas que atañen tanto a los órganos investigadores como a los tribunales. A partir del art. 14, prevé normas relativas al establecimiento de parámetros de obtención y conservación de pruebas que constan en las redes y sistemas, salvaguardando los derechos fundamentales de las personas.

La evidencia digital, a diferencia de la física es más susceptible de ser destruida y alterada; siendo así, la conservación de datos es vital para asegurar el éxito de una investigación. Es por ello que el Convenio se ocupa de establecer distintos métodos para asegurar la integridad de la evidencia digital, de manera tal que pueda ser incorporada a un expediente investigativo. Para ello la información debe ser verificada y autentificada por los entes investigadores, comprobando que los datos no hayan sido alterados. La forma tradicional de hacerlo es mediante lo que se denomina la "cadena de custodia"[26] (*chain of custody*), que implica que cada uno de los custodios secuenciales de la prueba debe asegurar que no la modificó y que la protegió ante la posibilidad de que otros lo hicieran.

En el caso de documentos o archivos electrónicos la cadena de custodia se puede mostrar mediante la existencia de protocolos o procedimientos internos, respecto del acceso a documentos o carpetas electrónicas con claves digitales, como son las encriptaciones en documentos (*hashing*), con *passwords* para acceder al documento que registran los cambios y

[26] La cadena de custodia se utiliza normalmente en materia penal para proteger muestras tomadas de algunas evidencias físicas, como lo son las de sangre, residuos de narcóticos o huellas dactilares para, eventualmente, generar una nueva prueba. La lógica deriva de asegurar que la sangre, cocaína o huella sean la misma que la obtenida en la escena del crimen y que ella no fue alterada en el momento en que se analizó.

los accesos que se tuvieron al mismo, y realizando copias mediante procesos espejo (*mirror image*).

En materia de prueba digital, los casos más comunes en los cuales la cadena de custodia puede ser puesta en duda son los relacionados con la confiscación de discos duros, computadoras y la subsecuente grabación de copias por parte de la autoridad[27], dado la facilidad con que la información pueda manipularse y editarse durante estos procedimientos.

Ahora bien, el Convenio establece distintas herramientas en los Títulos 2 a 5 de la Sección 2, las cuales tienen por objetivo la obtención de los datos, estas medidas son:

A.) La Conservación rápida de datos informáticos almacenados (art.16);

B.) Conservación y revelación parcial rápidas de los datos relativos al tráfico (art. 17);

C.) La orden de presentación (art. 18);

D.) Registro y confiscación de datos informáticos almacenados (art. 19);

E.) Obtención en tiempo real de datos relativos al tráfico (art.20);

F.) Interceptación de datos relativos al contenido (art. 21).

La redacción del Convenio es sucinta respecto de la conceptualización de cada una de las herramientas, de manera que dejó de lado la regulación en lo relativo a la incorporación y seguridad de la prueba dentro de los procesos investigativos. A continuación, se expondrá cada una de las herramientas contempladas en el Convenio, para ser incorporadas al derecho interno de cada uno de los países suscriptores.

i.- La Conservación rápida de datos almacenados

[27] MARÍN, Juan Carlos y GARCÍA, Guillermo. 2014. Problemas que enfrenta la prueba digital en los Estados Unidos de Norteamérica. Revista de Estudios de Justicia N°21. ISSN 0718-0853. 81 p.

Esta facultad se contempla en el artículo 16 del Convenio, y regula la posibilidad de que los entes investigadores soliciten la preservación de evidencia almacenada en dispositivos electrónicos, en particular cuando sean susceptibles de desaparecer o ser alterados *(periculum in mora*). Además, se establece la posibilidad de que la autoridad ordene al propietario o custodio de los datos, la preservación y protección de estos, por un plazo de hasta 90 días, renovables. A esto se suma la posibilidad de imponer la obligación de mantener el secreto sobre la actuación.

Esta herramienta fue creada con el fin de evitar que la información almacenada, ya sea en un dispositivo informático o en la "nube" sea intervenida. De esta manera, preservar el contenido de una cuenta de Dropbox, o Google Drive, por ejemplo, puede evitar que documentos, imágenes o vídeos, sean eliminados. De la misma forma, congelar o preservar una cuenta de correo, permitirá que el persecutor tenga acceso al historial de correos de un imputado, a los intercambios de comunicaciones; prueba fundamental, por ejemplo, en la investigación de un delito de cohecho.

ii.- Conservación y revelación parcial rápida de los datos relativos al tráfico

Esta medida está establecida en el artículo 17, que prevé que se pueda exigir a los proveedores de servicios de telecomunicaciones que realicen acciones de conservación y revelación de las comunicaciones electrónicas de un determinado usuario o un grupo de sus usuarios. Asimismo, procura asegurar que con posterioridad la información obtenida sea presentada ante la autoridad competente, de manera que la información sea tal que permita identificar tanto a los proveedores de servicios, como la vía por la que se ha transmitido.

Tanto la conservación rápida, como la conservación y revelación parcial rápida, tienen por objetivo la obtención y preservación de la información, ya sea de tráfico o almacenamiento, y puede tener como sujeto pasivo, tanto al propietario de la información (dueño del dispositivo), o bien a un proveedor de servicios, ya sea de tráfico o almacenamiento. En este último caso, el proveedor de la cuenta de *WhatsApp* o *Instagram*, en un delito por amenazas, es la empresa estadounidense *Facebook*, a quien deberá oficiarse para la información.

iii.- Orden de presentación

La Orden de Presentación consiste en la facultad que tiene la autoridad de un Estado miembro de la Convención para exigir ya sea a una persona natural presente en su territorio o a un proveedor que ofrezca servicios en un territorio, comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación dichos servicios.

El artículo señala además cuales son las exigencias que puede hacerse respecto al contenido de la información solicitada a los proveedores. De esta manera, conforme al numeral 3 del artículo 18, los datos entregados por la persona a quien se ordena efectuar la presentación deberán permitir determinar:

a) Tipo de servicio utilizado, y período en el cual se efectuó.

b) Identidad, dirección o situación geográfica y número telefónico del usuario. Así como cualquier otra información relativa a la facturación, pago y accesos.

c) Información relativa a la ubicación de los equipos.

De esta manera, el Convenio busca asegurar que mediante la información que entreguen los proveedores se pueda determinar la ubicación e identificación del usuario que está siendo investigado.

iv.- Registro y confiscación de datos informáticos almacenados.

Consiste en la posibilidad de las autoridades para registrar o tener acceso a:

- Un sistema informático, una parte de este o a los datos almacenados en él.
- Todo dispositivo de almacenamiento informático.

Este mecanismo contempla que la autoridad requirente tenga acceso a un sistema informático en específico, o bien que se tengan “motivos para creer” que los datos o información buscada

se encuentran en otro sistema al cual se puede acceder por medio del sistema inicial. Asimismo, el párrafo 3 permite a las autoridades la confiscación de los datos que se hayan obtenido durante las diligencias de registro, otorgando la posibilidad de:

a) Confiscar u obtener un sistema informático, una parte de este, o un dispositivo de almacenamiento.

b) Realizar y conservar una copia de los datos obtenidos.

c) Preservar la integridad de los datos pertinentes.

d) Hacer inaccesibles o suprimir dichos datos informáticos.

v.- Obtención en tiempo real de datos relativos al tráfico.

La particularidad de esta herramienta es que permite obtener o grabar por medios técnicos, o bien obligar a los proveedores de servicios, en la medida de sus capacidades, a grabar u obtener los datos relativos al tráfico asociados a **comunicaciones específicas** transmitidas por un sistema informático.

Los datos de tráfico, o metadatos, en una comunicación es la información que rodea el mensaje que se transmite, son un subproducto de las conexiones, que se concretará en función del tipo de comunicación[28]. En el acceso a internet y en el correo electrónico serán metadatos, tanto para el origen como para el destino de la comunicación, la identificación de usuario asignada, el nombre y la dirección del abonado o usuario al que se le ha atribuido una dirección de protocolo internet (IP); la fecha y hora de conexión y desconexión del servicio de acceso a internet; el servicio de internet utilizado; o la línea digital de abonado (DSL). Como se ve, estos

[28] Así, en una llamada telefónica, los metadatos serán: el número de teléfono de llamada, el nombre y dirección del abonado de origen, el número de destino y el nombre y dirección del abonado de destino, la fecha y hora del comienzo y fin de la comunicación, el servicio telefónico utilizado, y otros datos específicos de la telefonía móvil (la identidad internacional del abonado [IMSI] que llama y del que recibe la llamada; la identidad internacional del equipo móvil [IMEI], también del que llama y del que recibe la llamada; si el servicio es de pago por adelantado: fecha y hora de la primera activación del servicio y la etiqueta de localización o identificador de celda desde la que se haya activado el servicio).

datos accesorios a la comunicación detallan quién, cuándo, dónde y con quién se produce, sin entrar necesariamente en su contenido. En general estamos ante datos de abonados y usuarios que son tratados por los proveedores de comunicaciones para efectuar esta misma, pero que son susceptibles de ser usados de formas muy diferentes, a la vez que pueden agredir los derechos fundamentales. Téngase en cuenta que los metadatos[29] aluden a una comunicación concreta, siendo diferentes a otros datos o circunstancias personales que tendrán los operadores, pero que son autónomos y se hallan desconectados de una comunicación.[30] Este mecanismo es particularmente muy usado durante las investigaciones, con el objetivo de identificar la ubicación del autor, así por medio de la obtención de los datos relativos al tráfico vamos a poder identificar la dirección IP del dispositivo electrónico desde el que se emitió una amenaza o desde donde se subieron imágenes o videos a la web.

vi.- Interceptación de datos relativos al contenido.

Esta herramienta tiene por objetivo, la grabación u obtención de **contenido de comunicaciones específicas**. Opera con las mismas modalidades que la herramienta anterior, pero a diferencia de aquella, los datos relativos al contenido no identifican ubicación o direcciones IP desde las que se emitan o dirijan las comunicaciones, sino que permitirán obtener el mensaje comunicado. Esta herramienta es muy utilizada en las investigaciones relativas a tráfico de drogas, o personas, para identificar la información que se intercambian, o bien en las investigaciones de cohecho, donde se permite tener acceso al contenido de correos electrónicos en que se lleguen a acuerdos ilícitos.

4.- Salvaguardas.

El artículo 15 del Convenio de Budapest, titulado "Condiciones y Salvaguardas" impone a los Estados signatarios la obligación de asegurar por medio del derecho interno, que la aplicación

[29] Los metadatos son aquellos que describen el contenido, calidad, atributos de un archivo o información. Comúnmente se les denomina como los "datos de los datos", su importancia para la conservación de datos es que facilita el análisis de la información, la creación de informes, y mejora la eficiencia de los sistemas.

[30] FERNÁNDEZ Rodríguez, J. J. 2016. Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. Revista Española de Derecho Constitucional N°108. 96 p. [en línea] <http://dx.doi.org/10.18042/cepc/redc.108.03> [consulta: 1 de junio de 2020]

de las medidas contempladas en el Convenio garantice la protección de los derechos humanos y libertad de los particulares, en atención a los tratados internacionales suscritos en la materia. En esta área, el Convenio hace referencia al principio de proporcionalidad, el cual indica que las medidas contempladas en el Convenio no podrán sobrepasar los Derechos del individuo, más allá de lo que sea estrictamente necesario para la consecución del objetivo de la diligencia. El desarrollo del principio de proporcionalidad surge en Alemania durante principios del siglo XX, estableciendo ponderaciones que deben hacerse al momento de la aplicación de las normas jurídicas, en especial durante el ejercicio de la autoridad contra los derechos de las personas. Para Javier Barnes, el principio de proporcionalidad implica que "*la intervención pública ha de ser "susceptible" de alcanzar la finalidad perseguida, "necesaria" o imprescindible al no haber otra medida menos restrictiva de la esfera de libertad de los ciudadanos (es decir, por ser el medio más suave y moderado de entre todos los posibles —ley del mínimo intervencionismo—) y "proporcional" en sentido estricto, es decir, "ponderada" o equilibrada por derivarse de aquélla más beneficios o ventajas para el interés general que perjuicios sobre otros bienes, valores o bienes en conflicto, en particular sobre los derechos y libertades*."[31]

El fin que tiene la Convención es establecer mecanismos que faciliten las investigaciones penales, sin embargo, deja en manos de los Estados todo aquello relacionado con el resguardo y protección de los derechos humanos, estableciendo ciertos mínimos, que corresponden a los derechos derivados de tratados internacionales en la materia, entre los que cita; el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 1950; el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966, cuyo contenido tiene como principal enfoque el respeto por un debido proceso, un proceso racional y justo, derecho a la libertad de expresión y la privacidad. Nuestro

[31] BARNES, Javier. 1994. Introducción al principio de Proporcionalidad en el Derecho comparado y comunitario. Revista de Administración Pública. N°135. Septiembre-diciembre. 500 p. [en línea] <https://www.diarioconstitucional.cl/articulos/normas-de-principio-ponderacion-y-juicio-de-proporcionalidad> [consulta: 01 de junio de 2020]

país, solo es parte signataria del segundo de estos Tratados[32], el cual por mandato constitucional se encuentra incorporado en nuestro ordenamiento.

Respecto al principio de proporcionalidad citado por el Convenio, en nuestro país no se encuentra regulado expresamente en la Constitución, sin embargo, gracias a un trabajo jurisprudencial del Tribunal Constitucional (TC), se han logrado establecer criterios, y más específicamente un test que permite determinar si la afectación de alguno de los derechos consagrados en la Constitución es arbitraria: "*los límites al derecho consagrado en la Constitución deben, como ha señalado reiteradamente este Tribunal (Constitucional), pasar un examen de proporcionalidad; esto es, perseguir fines lícitos, constituir la limitación un medio idóneo o apto para alcanzar tal fin y resultar el menoscabo o limitación al ejercicio del derecho, proporcional al beneficio que se obtiene en el logro del fin lícito que se persigue*".[33] De esta manera, correspondería al juez de garantía determinar si durante la investigación se vulneraron los derechos de los imputados, y la autorización de diligencias que puedan afectarlos.

5.- Protocolo Adicional APCoC N° 189.

El Protocolo Adicional de la Convención de Cibercrimen, relativo a la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas computacionales *("Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems" o "APCoC")* es un tratado abierto a la firma para aquellos Estados que han ratificado el Convenio de Budapest, acordado en Estrasburgo el 28 de enero de 2003 y que comenzó a regir el 1 de marzo de 2013.

[32] Suscrito por Chile el 16 de diciembre de 1966, y promulgado por medio del Decreto 778, el año 1989.
[33] Considerando 21 de las sentencias roles N°1.182-08, de 22 de julio de 2008, 1.193-08, de 1 de agosto de 2008 y 1.201-08, de 13 de agosto de 2008. Citado por Arnold, Rainer; Martínez Estay, José Ignacio y Zúñiga Urbina, Francisco. El Principio De Proporcionalidad En La Jurisprudencia Del Tribunal Constitucional. Estudios constitucionales, vol.10, n.1. 2012. 67 p. ISSN 0718-5200. [en línea] <http://dx.doi.org/10.4067/S0718-52002012000100003>. [consulta: 01 de junio de 2020]

Sus objetivos son "primero, armonizar la ley penal sustantiva en la lucha contra el racismo y la xenofobia en internet y, segundo, mejorar la cooperación internacional en esta área"[34], el Comité de Ministros discutió la incorporación directa de estos objetivos a la Convención de Budapest, pero hubo aprensiones sectoriales por sus posibles efectos en la garantía de libertad de expresión, por lo que finalmente se postergó su implementación a medida que se siguió discutiendo la materia.

El Protocolo define por material racista y xenófobo "cualquier material escrito, cualquier imagen o cualquier otra representación de ideas o teorías, que abogan por, promueven o incitan el odio, la discriminación o la violencia, contra cualquier individuo o grupo de individuos, basado en raza, color, descendencia u origen nacional o étnico, como también en religión si es que se usa como pretexto para cualquiera de estos factores". Se incorpora religión en sentido estricto ya que el término se refiere a "El término refiere a convicciones y creencias. La inclusión de este término como tal en la definición conllevaría el riesgo de ir más allá del ámbito de este Protocolo"[35]. Sobre esta definición se establece la obligación de los Estados parte de adecuar su legislación con el fin de penalizar las siguientes conductas cometidas a través de sistemas informáticos: la diseminación de material racista y xenófobo; la amenaza de cometer seriamente un crimen con motivación racista o xenófoba; la distribución o habilitación de material que avale el negacionismo[36]; y la colaboración o incitación ilegítimas y a sabiendas en la comisión de alguno de estos delitos.

Actualmente, ha sido ratificado por la mayoría de los Estados europeos, teniendo como excepción; entre otros, a Reino Unido, Italia, Austria y Bélgica (estos 3 últimos lo suscribieron, pero no lo han ratificado). En América han adherido solo 2 Estados: Canadá (8 de julio de 2005) y Paraguay (30 de julio de 2018, conjuntamente a su ratificación del Convenio); de los cuales solo Paraguay ha ratificado, convirtiéndose en uno de los 3 Estados no europeos en ratificar el

[34] CONSEJO EUROPEO. Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. Estrasburgo. 2003. 1 p.
[35] CONSEJO EUROPEO. 2003. Op.Cit. 5p.
[36] *"Negacionismo, minimización grosera, aprobación o justificación de genocidios o crímenes contra la humanidad*". Ibid.

Protocolo N°189 además de Marruecos (el 29 de julio de 2018) y Senegal (el 16 de diciembre de 2018)[37].

Estados Unidos se ha restado expresamente de la firma de este protocolo por considerar que no se encontraría en el marco de su Constitución en relación al derecho de libertad de expresión. Según el Departamento de Justicia, en documento archivado sobre preguntas y respuestas frecuentes: "*Tal como la Convención principal, durante el proceso de negociación y diseño, los Estados Unidos buscaron comentarios y otros insumos de una variedad de grupos en representación de los intereses de Estados Unidos. En una serie de reuniones tenidas entre 2001 y 2002, representantes de los Departamentos de Justicia, Estado y Comercio se reunieron con representantes de la industria de tecnología y comunicaciones de EE.UU. y varios grupos de interés público para escuchar comentarios sobre las disposiciones del proyecto y para compartir información en el estado del protocolo. Como con la Convención principal, el Consejo de Europa hizo numerosos proyectos disponibles para el público. Los Estados Unidos no creen que la versión final del protocolo sea consistente con sus garantías constitucionales. Por esta razón, los Estados Unidos ha informado al Consejo de Europa que no va a formar parte del protocolo.*"[38] Lo señalado por el Departamento de Justicia de EE. UU., explica el motivo por el que el protocolo no ha tenido la misma acogida internacional que el Convenio a nivel internacional en consideración a la influencia internacional de EE.UU. De todas maneras, la ausencia de documentos oficiales traducidos en idiomas más allá del francés, alemán, ruso e inglés es una barrera importante que el mismo Consejo de Europa podría fácilmente sortear para fomentar su discusión, considerando especialmente que países de otras lenguas ya lo han adoptado a pesar de la ausencia de localización oficial.

En conclusión, y a modo de reflexión, el protocolo busca regular una materia bastante delicada, referente a la utilización de las redes para fomentar el odio y discriminación, práctica que

[37] CONSEJO EUROPEO. Lista oficial de adherencias y ratificaciones. [en línea] <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=0mbpKdij> [consulta: 1 de junio de 2020]

[38] U.S. DEPARTMENT OF JUSTICE. Frequently asked question and answers Council of Europe Convention on Cybercrime. [en línea] <https://web.archive.org/web/20060209153034/http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QE1> [consulta: 01 de junio de 2020]

lamentablemente va en aumento durante los últimos años y que construye un discurso de odio generalizado fácil de replicar, protegido en el anonimato on-line y la falta de responsabilidad de cualquier ámbito. Sus efectos, en la mayoría de los casos, son difusos, pero muchas veces se traduce en acciones concretas contra ciertos individuos o en la afectación cierta en los derechos básicos de éstos mismos. En cualquiera de los casos, es un elemento nocivo que no se puede aceptar en una sociedad democrática sin poner en peligro las bases de la misma tolerancia en la que falazmente se suele apoyar.

El problema que acarrea la escasa adopción del Protocolo es un tema importante a analizar, donde el rechazo expreso de Estados Unidos es un elemento no menor, siendo uno de los países de mayor acceso a internet a nivel mundial, donde las cifras[39] de ciberacoso en la etapa de la adolescencia son muy altas, y según distintos estudios[40] uno de los principales motivos de suicidio adolescente en este país, fomentado por la diversidad étnica, racial y religiosa que presenta EEUU; el conflicto que se plantea respecto la primacía del derecho a la libertad de expresión, frente a la no discriminación es un tema de estudio aparte; sin embargo, no hay que dejar de mencionar que la naturaleza de internet es el lugar perfecto para la proliferación y masificación de mensajes de odios a comunidades y grupos de población específicos, todo bajo el alero del anonimato. El derecho penal en general ha sido históricamente reticente a la tipificación y sanción de discursos de odio e insultos[41]; sin embargo, hoy gracias a la "viralización" de contenidos, y la facilidad de que miles de usuarios sean testigos de un *tuit,* o una publicación en alguna red social en cuestión de segundos, cabe hacerse la pregunta de si los Estados están dispuestos a dejar pasar la posibilidad de regular y sancionar conductas como éstas. Chile, el año 2012 dictó la ley 20.609 que establece medidas contra la discriminación, también conocida como "Ley Zamudio", que incorpora como agravante de la responsabilidad

[39] "El Centro de Investigación de Ciberacoso informa que el 33.8% de los estudiantes de secundaria y preparatoria en los Estados Unidos han sido víctimas de alguna forma de acoso cibernético, ya sea a través de comentarios hostiles o hirientes en línea o por haber recibido amenazas de violencia por medio de dispositivos digitales". [en línea] <https://www.websitebuilderexpert.com/blog/us-state-biggest-cyberbully/> [consulta: 1 de junio de 2020]

[40] HINDUJA, Sameer & PATCHIN, Justin. 2008. Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying. Journal of School Violence. Pp 1-14.

[41] Las injurias y calumnias en Chile se encuentran tipificadas en los artículos 416 y 412 del Código Penal, respectivamente, cuyas penas asignadas tienen como máximo asignado la reclusión menor en su grado medio.

penal[42] el *"Cometer el delito o participar en él motivado por la ideología, opinión política, religión o creencias de la víctima; la nación, raza, etnia o grupo social a que pertenezca; su sexo, orientación sexual, identidad de género, edad, filiación, apariencia personal o la enfermedad o discapacidad que padezca".* Norma de aplicación general que permite el aumento de las penas en la comisión de los delitos motivados por odio contra determinadas personas; el problema es que esto no va de la mano, nuevamente, con una sanción especifica al ciberacoso, sin perjuicio de que el proyecto que sanciona esta conducta en nuestro país se encuentra en tramitación en el Congreso[43], desde el año 2018.

Finalmente hay que señalar que el derecho de la libre expresión no está puesto en tela de juicio por el Protocolo, pero dado el contenido en sí de este derecho, es que no es posible amparar un discurso de odio y discriminación arbitraria que sea manifestado y masificado por la Red; las consecuencias no son un misterio, ataques motivados por la religión o por la orientación sexual abundan, y es deber de los Estados hacerse cargo no solo de la educación en estas materias sino también de sancionar a quienes las promuevan o difundan.

Por esto, la discusión en torno al Protocolo nos parece un gran aporte para avanzar en la regulación de la materia; sin embargo, se debe ser sumamente cuidadosos para no establecer herramientas peligrosas que atropellen las garantías constitucionales de los ciudadanos. Algunas de las herramientas contempladas en el Protocolo parecieran peligrosas o desproporcionales en estos términos, por lo que habría que realizar un análisis complejo sobre sus límites. El mismo Protocolo contempla la posibilidad de reservar varias de las disposiciones más polémicas, por lo que en todos los casos debería procederse a su discusión informada y abierta a la sociedad civil.

6.- Cooperación Internacional.

[42] Artículo 12, numeral 21 Código Penal.
[43]CÁMARA de diputados. Boletín 12022-04. [en línea] <https://www.camara.cl/pley/pley_detalle.aspx?prmID=12550&prmBoletin=12022-04> [consulta: 01 de junio de 2020].

La cooperación jurídica internacional, puede definirse como un mecanismo mediante el cual un Estado solicita la colaboración de otro Estado a fin de resolver diferentes aspectos de un proceso judicial[44]. En este sentido, las normas de cooperación entre Estados se fundan en la necesidad de obtener un resultado determinado en territorio de otro país, ya sea la práctica de una diligencia, obtención de una declaración o de alguna otra evidencia útil para ser incorporada en una investigación.

La cooperación jurídica internacional, es una solución a los problemas de soberanía y jurisdicción que se produciría en aquellos casos en que en el marco de una investigación que requiera practicar una actuación en territorio extranjero, ya sea, por parte de los tribunales o la policía de una nación. De esta forma, mediante la coordinación especializada de organismos públicos y privados se llevan a cabo las diligencias solicitadas por un determinado Estado[45] sin pasar a llevar la soberanía, y permitiendo que los resultados obtenidos, sean incorporados en un proceso, por tratarse de un mecanismo reconocido interestatal e internacionalmente.

El Convenio de Budapest, reconoce tanto en su preámbulo, como en su cuerpo la importancia y necesidad de intensificar los vínculos de cooperación internacional, así lo expresan los párrafos 7 y 8 del preámbulo, que señalan:

"*Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de información*"

"Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal."

[44] MONTENEGRO, María Luisa. Cooperación Internacional: Tramitación, obtención de pruebas, e incorporación de pruebas y evidencias. Revista Jurídica Ministerio Público N°70. 64 p.

[45] Es importante señalar que quien eleva la solicitud de asistencia legal mutua es un determinado Estado, y no una entidad determinada de este, y a su vez va dirigida a otro Estado, el cual determinará la manera y organismo óptimo para llevar a cabo la diligencia solicitada.

Así también, el Convenio destina un capítulo (III) exclusivamente dedicado a la cooperación internacional, el cual cuenta con dos secciones, la primera de ellas referida a los "Principios Generales de la Cooperación", y la segunda titulada "Disposiciones Específicas"; la que aborda las Medidas Provisionales, la Asistencia Mutua en relación con los Poderes de Investigación y el establecimiento de una Red 24/7 que asegure una asistencia eficaz entre las partes.

El artículo 23, referido a los principios generales relativos a la cooperación internacional, dispone la obligación de las partes contratantes de cooperar en la **mayor medida posible**, lo que implica la mayor colaboración recíproca, que permita la rápida y eficiente entrega de asistencia por parte de los Estados, y que como ya hemos visto, es aplicable tanto para aquellos delitos de carácter informático, como aquellos delitos tradicionales cuyas evidencias se puedan encontrar almacenadas en dispositivos tecnológicos, o bien que se requiera la práctica de una diligencia en territorio extranjero que será facilitada mediante la utilización de sistemas informáticos. La asistencia mutua, o MLA, por su sigla en inglés (*mutual legal assistance*) es el camino formal por el cual los Estados requieren y proporcionan asistencia en la obtención de pruebas ubicadas fuera de las fronteras de su país y que asiste en investigaciones o procedimientos criminales en otro Estado. El Estado que hace la solicitud generalmente se conoce como el "Estado requirente", mientras que el estado al que se hace la solicitud es el "Estado requerido". La Asistencia Legal Mutua fue diseñada para la reunión de evidencia, no servicios de inteligencia u otra información[46]. Para esto existen otros medios de carácter administrativo encargados de coordinar con la institución correspondiente en otros Estados, comunicación que se lleva a cabo a través de la autoridad central designada para tal efecto.

Asimismo, dentro de las facultades que tienen los Estados parte, se encuentra la posibilidad de en caso de urgencia formular solicitudes de asistencia mutua a través de medios de comunicación rápidos como el correo electrónico, siempre que estos ofrezcan niveles óptimos

[46] COUNCIL OF EUROPE. Mutual Legal Assistance Manual. Belgrado, Serbia. ISBN 978-86-84437-57-2. 2013. 9 p. [en línea] <https://rm.coe.int/mutual-legal-assistance-manual-eng/1680782927> [consulta: 01 de junio de 2020]

de seguridad (artículo 25 N°2), esta norma en la actualidad tiene aplicación amplia y se materializa a través de la Red 24/7 que se analizará más adelante.

Doble incriminación[47]*:* de acuerdo con lo establecido en el numeral 5 del artículo 25, se establece los casos en que la Parte requerida podrá condicionar la asistencia cuando no exista doble incriminación, sin embargo, se entenderá que existe doble incriminación igualmente en aquellos casos en que aun sin coincidir la tipificación o categoría delictual se encuentre contemplado a nivel de delito en el país requerido.

Autoridad Central: La autoridad central; para estos efectos, se podría definir como aquella institución establecida en el Convenio de Budapest, en su artículo 27, como la encargada de enviar y responder las solicitudes de asistencia mutua, de ejecutarlas o remitirlas a las autoridades competentes para su ejecución, siempre y cuando no exista regulación entre los Estados. La Convención habla de una o más autoridades centrales, que serán nombradas por el Estado Parte al momento de firmar, depositar el instrumento de ratificación, aceptar o adherir al Convenio.

Cabe señalar que la autoridad central no es una institución única del Convenio de Budapest, sino que es parte de la tendencia moderna en materia internacional de centralizar los requerimientos entre puntos de contactos determinados, como expondremos a continuación.

Designación: La determinación de la autoridad central depende en exclusiva del Estado Parte del Convenio, no se establece limitación alguna a la naturaleza de ésta ni tampoco al número. Se alienta sí, según el informe explicativo, a la determinación de una única autoridad para mantener el objetivo de eficacia en la tramitación de solicitudes. Esta designación la debe realizar el Estado al momento de la firma o depósito de su instrumento de ratificación,

[47] La doble incriminación en cooperación internacional, lo encontramos recogido e distintos cuerpos normativos, así por ejemplo, el artículo 2.1 del Convenio europeo de extradición de 1957 señala "*Darán lugar a la extradición aquellos hechos que las Leyes de la Parte requirente y de la Parte requerida castiguen, bien con pena privativa de libertad o medida de seguridad privativa de libertad cuya duración máxima sea de un año por lo menos, bien con pena más severa";* siendo reconocido hoy como un principio general en materia de cooperación internacional, recogido por ejemplo, en el Acuerdo sobre extradición entre los estados parte del MERCOSUR y la república de Bolivia y la república de Chile (art. 2.3)

aceptación, aprobación o adhesión, cada Parte debe comunicar al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas.

Registro: El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro. Respecto a este punto, se establece un registro internacional precisamente para evitar los vaivenes diplomáticos y darle permanencia a la institución de autoridad central, al que cualquier autoridad central o Estado parte pueda acudir para efectos de realizar las solicitudes de asistencia, estando obligadas las partes a mantener la información al día.

Funciones y atribuciones: Las autoridades centrales están encargadas de enviar las solicitudes de asistencia mutua como también de responder las solicitudes recibidas. Además, se establece la responsabilidad de ejecutar las mismas solicitudes recibidas o de remitirlas a las autoridades competentes para su ejecución. Todo lo que se refiere a estas solicitudes se realiza mediante la comunicación directa entre las autoridades centrales de los Estados parte.

Procedimiento de solicitud: Sobre la forma y contenido de la solicitud, no se establece regulación particular para así mantener un grado de flexibilidad según la situación concreta y respetar a su vez las formas que determinen los Estados parte, que a falta de acuerdo al respecto deberán obedecer el derecho de la Parte requerida en lo que se refiere a la provisión de la solicitud. Así, debe estar en el idioma del Estado requerido y atender a la institucionalidad y normativa de éste.

Sin embargo, lo anteriormente señalado no se debe confundir con lo establecido en el párrafo 3 del artículo 27 que establece que el procedimiento de la solicitud se *ejecutará* de conformidad a lo dispuesto por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida. A lo que apunta esto último es a la eficacia de las gestiones que motivan la solicitud. En efecto, uno de los objetivos que se buscan mediante estas solicitudes es que el resultado pueda ser presentado ante la justicia local y para esto se debe cumplir con la normativa procesal de la Parte requirente; si no, podría darse que

la gestión solicitada se fuera a ejecutar según lo determinado por la Parte requerida de buena fe pero luego resultare que por no cumplir con la normativa del Estado requirente lo obrado resulte inútil por la imposibilidad de incorporar esta prueba en juicio, por ejemplo. Así, la solicitud debe efectuarse respetando la legislación del Estado requerido, su autoridad central y sus competencias, pero el procedimiento debe estar configurado para ser eficaz a la luz de la normativa procesal del Estado requirente.

Finalmente cabe destacar que la solicitud puede contemplar trámites o formas que no se encuentren regulados en la normativa del Estado requerido, lo cual no significa que pueda ser denegada por esta razón. Así, se podría solicitar que la declaración de un testigo sea realizada de forma verbal y traspasada por escrito a un documento firmado por un ministro de fe y el mismo declarante, cuando la regulación de la Parte requerida no establezca este requisito para la declaración. En este caso la requerida no podría rechazar la solicitud señalando que según su legislación la declaración del testigo deba realizarse de otra manera. Lo relevante es que la solicitud no contraríe los principios jurídicos del Estado requerido, por ejemplo, se podría rechazar la solicitud al Ministerio Público de que se efectúen apremios con el fin de obtener respuestas concretas a un interrogatorio, toda vez que atentaría contra la presunción de inocencia y el derecho a guardar silencio.

Denegación de la solicitud: La autoridad central requerida podrá denegar la solicitud de conformidad al artículo 25 del Convenio, es decir según “las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables”. Por otra parte, el párrafo 4 del artículo 27 incluye motivos de perjuicio a la soberanía, la seguridad, al orden público o a otros “intereses esenciales” del Estado. Otro caso de denegación corresponde a un delito considerado, por la Parte requerida, como un delito político o conexo. Se indica además que la Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

El párrafo 5 establece la posibilidad de aplazar la actuación de una solicitud para evitar perjuicios en investigaciones o procedimientos. En lo que a plazos se refiere, no hay una regulación específica por parte del Convenio de Budapest, por lo que se deben seguir las normas procedimentales señaladas previamente. Tanto el aplazamiento como la denegación de solicitudes debe ser fundada por el Estado requerido.

Finalmente, a pesar de lo señalado en relación con la posibilidad de denegar la solicitud internacional en ciertos casos, hay que recordar la relevancia que tiene la asistencia mutua en esta materia. Al establecerse una causal amplia de denegación de solicitudes se ataca precisamente este objetivo al permitir la denegación por consideraciones internas basadas en intereses esenciales. Sin embargo, el mismo Convenio en su párrafo 6 establece: "*6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias*". De esta forma, la denegación de la solicitud debe ser un caso absolutamente excepcional incluso por la causal de "intereses esenciales" del Estado requerido y previamente éste debe estudiar de forma conjunta con el requirente la manera en la que se podría cumplir la solicitud.

Confidencialidad de la solicitud: El párrafo 8 permite la posibilidad de solicitar la confidencialidad de la presentación y objeto de cualquier solicitud. En caso de que se deniegue este punto, el requerido deberá informar sin demora y el requirente deberá determinar si la solicitud debe ser ejecutada de todas maneras.

Solicitud directa en caso de urgencia: El párrafo 9 establece la posibilidad de obviar la autoridad central y dirigirse directamente a la autoridad judicial de un Estado requerido por la autoridad judicial del Estado requirente. Para la aplicación de esto, se debe estar en un caso de *urgencia*, es decir que el retraso en la gestión implique un riesgo para el procedimiento en sí o para el interés esencial de alguna de las Partes. Estas solicitudes pueden realizarse mediante la Organización Internacional de Policía Criminal (Interpol) y en cualquier caso se remitirán copias de la solicitud a las autoridades centrales de las Partes. Incluso, en caso de que las medidas

solicitadas no sean coercitivas podrán ser solicitadas directamente entre autoridades competentes. Al momento de la firma o depósito del instrumento de ratificación, aceptación aprobación o adhesión, el Estado podrá informar al Secretario General del Consejo de Europa de que estas solicitudes deban dirigirse a su autoridad central, facultad que no fue utilizada por nuestro país.

Información espontanea: una de las mayores muestras de asistencia legal contemplada en el Convenio es el artículo 26, que contempla la institución de la información espontánea, que consagra la posibilidad de que, sin un requerimiento previo, un Estado que obtenga información en el marco de sus investigaciones, la que podría ser útil para la investigación de algún otro Estado, se la entregue.

La entrega de esta información puede ser condicionada por el Estado emisor, para que sea utilizada bajo ciertas condiciones, por ejemplo, la confidencialidad. A modo de ejemplo, en el marco de una investigación por delitos de estafa en un país extranjero, mediante escuchas telefónicas se obtiene la información de que los involucrados estén desviando dinero a nuestro país, y que eventualmente podría estarse cometiendo el mismo delito en Chile.

Esta información se comunica a la autoridad central en nuestro país, la cual determinará la actuación si está de acuerdo con las condiciones impuestas por el país que proporciona la información.

7.- Red 24/7.

El concepto de Red 24/7 no es exclusiva del Convenio de Budapest, sino que lo encontramos en distintos acuerdos internacionales[48], en los que se hace esencial la coordinación y cooperación de Estados y sus instituciones, para el buen funcionamiento y aplicación del tratado.

[48] Red países G8, Red Interpol, Red de CSIRT's (computer security incident response team).

De esta manera, y con el fin de asegurar una respuesta rápida y oportuna de evidencia e información en el marco de investigaciones y procedimientos de cibercriminalidad es que los países Partes del Convenio de Budapest se han comprometido a designar un punto de contacto[49] que sea localizable 24 horas al día, 7 días a la semana, tal como indica su nombre, el cual permita garantizar asistencia inmediata. Ya hemos mencionado lo falible que puede resultar la información digital, es por ello que la preservación de la información y la forma en que deben llevarse a cabo las investigaciones en materia de ciberdelitos exige establecer mecanismos que permitan obtener resultados oportunos.

El artículo 35 contempla el establecimiento de la Red y punto de contacto por el Estado parte, ya sea que directamente o facilitando los medios correspondientes, entreguen la asistencia que señala el numeral 1 del artículo mencionado:

- En primer lugar, el asesoramiento técnico,
- En segundo término; La conservación de datos, y obtención de pruebas,
- Y la localización de sospechosos.

En el caso chileno, la Unidad de Colaboración Internacional y Extradiciones (UCIEX), como punto de contacto de la Red 24/7 es la encargada y capacitada para responder asesorías técnicas de otros Estados, junto con las demás unidades especializadas de la Fiscalía Nacional, relativas a las investigaciones penales que tengan alguna vinculación o efecto en nuestro país, de la misma manera es la encargada de dirigirse a los Fiscales, para que estos encarguen a los funcionarios policiales[50] la práctica de diligencias y localización de personas, en el territorio de nuestro país.

[49] En el caso chileno, el punto de contacto corresponde a la Unidad de Cooperación internacional y Extradiciones (UCIEX) de la Fiscalía Nacional del Ministerio Público de Chile. La UCIEX, es una Unidad de apoyo a la labor del Ministerio Público, compuesta por abogados asesores, especializados en materia de Cooperación Internacional, sin embargo, al no tener el rol de Fiscal no pueden encargar directamente la práctica de diligencias a las Policías.
[50] Carabineros de Chile y Policía de Investigaciones de Chile.

Los casos de cooperación internacional, mediante las plataformas 24/7 tienen la particularidad de que mediante un contacto directo entre los organismos encargados de las investigaciones en distintos países, circule la información que permita la ubicación de sospechosos; así por ejemplo, en el año 2009, en España, el cantante David Bisbal, denunció estar siendo víctima de una extorción de parte de desconocidos[51], que habrían ingresado de manera ilícita a su correo electrónico, y del que habrían obtenido información personal e imágenes intimas, las que amenazaban con subir a la *web* a cambio de una alta suma de dinero; el cantante puso la denuncia ante el Juzgado de Almería, el cual solicitó a la Guardia Civil española (símil de Carabineros de Chile) se iniciara una investigación para determinar el origen de dichas amenazas; mediante la coordinación de la policía española, se logró determinar que la dirección de acceso a la cuenta de correo de la víctima, se encontraba en República Dominicana, lugar donde fueron detenidas las personas involucradas; este es un caso en que la coordinación entre países de distintas regiones fue esencial para la detección, captura y sanción de los autores del delito.

8.- Rol de los Proveedores de Servicios.

A diferencia de otras investigaciones, acceder a las pruebas digitales implica dirigirse principalmente al sector privado, que es el que opera y mantiene en gran parte la infraestructura de Internet. Por ello, es fundamental colaborar entre las distintas partes interesadas a fin de abordar las nuevas amenazas cibernéticas[52].

Más allá de determinar si alguno de los proveedores de servicios de telecomunicaciones e internet pueden ser responsables ya sea civil o penalmente por los delitos cometidos a través de la Red, nos enfocaremos en el rol que le asigna el Convenio de Budapest y cómo los Proveedores de servicios son un factor esencial al momento de la investigación.

[51] EL MUNDO. Cuatro detenidos en la República Dominicana por extorsionar a Bisbal. <https://www.elmundo.es/elmundo/2009/01/13/cultura/1231842140.html. [consulta: 01 de junio de 2020]

[52] INTERPOL. Estrategia mundial contra la Ciberdelincuencia. 2017. [en línea] <https://www.interpol.int/ar/content/download/5586/file/Summary_CYBER_Strategy_2017_01_SP%20LR.pdf?inLanguage=esl-ES.> [consulta: 01 de junio de 2020]

El término "**proveedor de servicios**", según señala el Informe explicativo del Convenio de Budapest[53], abarca a una amplia categoría de personas que desempeñan un papel particular con respecto a la comunicación o el tratamiento de los datos a través de los sistemas informáticos. En el numeral i) de la definición, se aclara que quedan comprendidas todas las entidades tanto públicas como privadas que ofrecen a los usuarios la posibilidad de comunicarse entre sí, ya sea que ofrezcan su servicio gratuitamente o a cambio de un arancel. En el numeral ii) de la definición se aclara que el término "proveedor de servicios" abarca también a aquellas entidades que procesen o almacenen datos en nombre de las personas mencionadas en el inciso i y para los usuarios.

A mayor abundamiento, de acuerdo con lo establecido por la Subsecretaría de Telecomunicaciones de Chile (SubTel)[54] se entenderá por:

Proveedor de Acceso a internet o ISP, la persona natural o jurídica que presta el servicio de acceso a Internet, de conformidad a la ley y su normativa complementaria.

Proveedor de Contenido, la persona natural o jurídica que pone a disposición de los usuarios contenido y/o aplicaciones en Internet a través de medios propios o de terceros.

De esta forma, ambas definiciones quedan comprendidas dentro del concepto del Convenio de Budapest, por lo tanto, en el marco de una investigación por un ciberdelito, conforme al Convenio podríamos solicitar, por ejemplo, a VTR o a Facebook Inc., su colaboración, como proveedor de acceso a internet y proveedor de contenidos respectivamente, en aquellas diligencias que el órgano a cargo de la investigación solicite. Por ejemplo, identificación de la dirección IP desde la cual se conectó uno de los imputados, o bien el congelamiento de datos de la cuenta Facebook, en específico respecto al historial de conversaciones mantenidas por medio de la plataforma.

[53] Apartado 26 y siguientes. 8 p.
[54] Mediante su resolución exenta N° 1.483, de 22 de octubre de 1999, para fijar el procedimiento y plazo para establecer y aceptar interconexiones entre Proveedores. Artículo 1.

De esta forma, de los proveedores es el de aportar, desde el área técnica, con la información almacenada para las investigaciones penales que involucren evidencia digital a la cual ellos tienen acceso como custodios. En específico las normas del Convenio tienen por fin asegurar la información y datos almacenados, para lo cual se insta a los Estados parte a desarrollar cuerpos normativos que aseguren la cooperación de los proveedores a las investigaciones. Sin embargo, esto no es muy lejano a lo que contempla nuestra legislación, ya que dentro de las diligencias que pueden realizarse en las investigaciones por parte de las policías, previa autorización del Juzgado de Garantía está la posibilidad de la interceptación de comunicaciones (artículo 21).

Los problemas que se plantean respecto el papel de los proveedores de servicios son muchos, entre ellos, la vulnerabilidad y exposición de nuestros datos e información en la web, la vulneración al derecho a la privacidad de las comunicaciones y la intimidad, problemas técnicos asociados a la implementación de la medida, la responsabilidad de los proveedores por el manejo y custodia de la información, los plazos de almacenamiento de los datos e información, entre otros. El Convenio establece que, una vez realizado el congelamiento, los plazos no sean superiores a 90 días, prorrogables.

El Convenio en su artículo 15 se refiere a las salvaguardas y condiciones que debe adoptar cada Estado parte para que en el ejercicio de las herramientas previstas en el convenio no se vulneren los derechos de los ciudadanos. Si bien deja a los Estados la regulación de contenido y forma en que las instituciones, como el Ministerio Público y las policías, en el caso chileno, llevarán a cabo estas medidas, las cuales también pueden provenir de Estados extranjeros, mediante la cooperación internacional. Al respecto, debemos considerar que, en nuestro caso, el Ministerio Público generalmente operará como requirente, dado que los principales proveedores de servicios, y compañías generadoras de páginas de acceso y aplicaciones móviles, se encuentran con sede fuera de nuestro país, e incluso fuera de nuestra región, por lo cual utilizando la plataforma Red 24/7 a través de su autoridad central la UCIEX se comunicará con la autoridad central correspondiente al Estado sede en que se encuentra el

proveedor que cuenta con la información que sirve de evidencia en la investigación llevada en nuestro país.

CAPÍTULO II: ADOPCIÓN DEL CONVENIO EN CHILE Y APLICACIÓN EN EL SISTEMA PROCESAL.

1.- Regulación de la ciberdelincuencia en Chile

a.- Aspectos sustantivos

Nuestra legislación se encuentra desactualizada en lo que se refiere al tratamiento sistemático de la ciberdelincuencia. El Código Penal no contiene un apartado sobre delitos informáticos y salvo contadas excepciones[55], no ha sido modificado a propósito de los desafíos que impone la masificación de las tecnologías de comunicación.

La regulación específica se ha realizado mediante leyes especiales. La principal es la Ley 19.923 del año 1993 que "*tipifica figuras penales relativas a la informática*". Esta ley, mediante sus 4 artículos, contiene las figuras penales de: destrucción de un sistema informático; acceso ilícito a datos informáticos; destrucción o alteración de datos informáticos y revelación o difusión de datos informáticos. Para determinar el bien jurídico protegido por esta ley, debemos recurrir a su historia, donde se consagra como "*la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan*"[56]. Si bien nos parece una buena aproximación sobre la materia, es importante considerar que esto es sin perjuicio de los bienes jurídicos protegidos asociados a cada figura, tales como el derecho de propiedad o la protección de la fe pública.

Un elemento común de estas figuras es la exigencia de un elemento subjetivo del tipo, siendo el de una "conducta maliciosa" en 3 de los 4 ilícitos, o de "*el ánimo de apoderarse usar o conocer indebidamente*" en el delito de acceso ilícito a información o espionaje informático del artículo 2. De esta forma, se exige el ánimo positivo de producir daño a otro o de

[55] Tales como las modificaciones realizadas por la Ley 20.526 que "sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil" al artículo 366 quáter y quinquies del Código, en relación al soporte y contenido de lo que se entiende por "material pornográfico".

[56] BIBLIOTECA del Congreso Nacional de Chile. Historia de la Ley N° 19.923. Delito informático. Primer Trámite Constitucional: Cámara de Diputados, Moción Parlamentaria. 4p.

beneficiarse mediante estas conductas; requisito equivalente en la mayoría de los casos al dolo directo, lo que se incorporó en la tramitación legislativa de su proyecto original[57].

Otra ley de contenido sustantivo en materia de ciberdelincuencia es la Ley 20.009 de 2005 que "limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas". Esta ley cubre materias de responsabilidad del tarjetahabiente frente al extravío, hurto o robo de su tarjeta, estableciendo que se le exime de toda responsabilidad a partir del momento en que dé aviso al banco emisor de la tarjeta. Además, en su artículo 5° establece el delito de uso fraudulento de tarjeta de crédito o débito que se comete mediante cualquiera de las conductas que describe[58] sobre falsificación de tarjetas o comercialización de éstas.

Actualmente, frente al avance de las tecnologías de clonación de tarjetas por banda magnética, en la mayoría de los casos se hace imposible para la víctima dar aviso previo a la comisión del fraude. Por este motivo se aprobó recientemente el proyecto de Ley Boletín 11078-03; hoy la Ley 21.234, que limita la responsabilidad de los titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude. Esta ley utiliza el concepto de "medio de pago" para regular también las transferencias electrónicas; establece deberes concretos de los emisores para limitar su responsabilidad (acreditar identidad de quien realiza transacciones); acorta los plazos de restitución de fondos del banco al usuario a 5 días hábiles (o 12 si son montos superiores a 35 UF); prohibir el cobro de seguros o comisiones especiales para la protección frente a fraudes; establece las conductas que constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas[59] e incluso extiende las medidas

[57] Presentado por moción parlamentaria del diputado José Antonio Viera Gallo con fecha 16 de julio de 1991.

[58] a) Falsificar tarjetas de crédito o débito.
b) Usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas.
c) Negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o sustraídas.
d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular.
e) Negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior.
f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

[59] Artículo 7.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

de interceptación de comunicaciones en caso de que sea imprescindible y existan sospechas fundadas de la intervención de una agrupación de 2 o más personas para cometer estos delitos; entre otras disposiciones.

En lo que se refiere a delitos contra la indemnidad sexual por medios informáticos, nuestro Código Penal sanciona en su artículo 366 quáter la exhibición de acciones sexuales o material pornográfico a un menor de edad. Además, penaliza al que determinare a un menor a realizar acciones de carácter sexual o a entregar imágenes de contenido sexual. Estas figuras aplican a víctimas menores de 14 años, para menores de 18 años procede; a su vez, solo en cuanto se acredite que el actuar fue realizado con fuerza o intimidación, en abuso de las condiciones desfavorables de la víctima (contenidas en el artículo 363) o con amenazas. Además, se señala expresamente que las penas descritas se aplicarán también cuando los delitos sean cometidos a distancia, por cualquier medio electrónico.

Respecto a la tipificación de pornografía infantil, nuestro Código Penal la establece en su artículo 366 quinquies[60]. Se castiga la producción del material, cualquiera sea su soporte. Se define material pornográfico de menores como "*toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes*

a) Falsificar tarjetas de pago.
b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.
c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.
d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.
e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago y claves o demás credenciales de seguridad o autenticación para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.
f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.
g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.
h) Obtener maliciosamente, para sí o para un tercero, el pago total o parcial indebido, sea simulando la existencia de operaciones no autorizadas, provocándolo intencionalmente, o presentándolo ante el emisor como ocurrido por causas o en circunstancias distintas a las verdaderas.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

[60] Artículo incorporado en la Ley 19.927 de enero de 2004 y complementado por la Ley 20.526 de agosto de 2011.

genitales con fines primordialmente sexuales, o toda representación de dichos menores en que se emplee su voz o imagen, con los mismos fines". El destacado es nuestro e ilustra la amplitud de la norma ya establecida en nuestra legislación, por lo que llama la atención que nuestro país se haya reservado la aplicación del artículo 9 párrafo 2 literales b y c del Convenio de Budapest que establecen "*2. A los efectos del párrafo 1 anterior, se entenderá por "pornografía infantil" todo material pornográfico que contenga la representación visual de: (…) b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.*"

La reserva adoptada por nuestros legisladores (propuesta por el ejecutivo) se vuelve confusa con lo ya dispuesto por nuestro Código Penal, toda vez que lo penado en el Convenio de Budapest estaría penado a su vez por la norma interna ya que "toda representación" incorpora ambos casos, lo que evidencia una falta de prolijidad o claridad en la tramitación del Convenio.

Finalmente, en materia de propiedad intelectual, debemos apuntar a lo dispuesto por la Ley 17.336 que protege los derechos patrimoniales y morales que protegen el aprovechamiento, la paternidad y la integridad de una obra de inteligencia creada por un autor en dominios literarios, científicos o artísticos, cualquiera sea su forma de expresión. En su capítulo II de las acciones y procedimientos establece los tipos penales con sanciones de multa o reclusión sobre quienes atenten contra la propiedad intelectual; además de sanciones civiles, con sus respectivos procedimientos, los que podrían ser aplicables a parte importante del tráfico nacional de internet gracias a la amplitud de la terminología empleada. En su capítulo III contempla una limitación de responsabilidad de los prestadores de servicios de internet: Se establece que; cumpliendo con una serie de condiciones, no se les hará responsable de indemnizar daños por perjuicios causados en los derechos de los usuarios dentro de las redes bajo su custodia, "sin perjuicio de las normas generales sobre responsabilidad civil aplicables". Las garantías establecidas son parte del principio de neutralidad en la red según el cual los proveedores de servicios no pueden gestionar el tráfico de datos con criterios selectivos, es decir no pueden discriminar según origen o contenido de la información. Este principio; como

también las actuales sanciones y procedimientos, fueron desarrollados e incorporados mediante la Ley 20.453 de 2010, complementada por su reglamento en Decreto Supremo de Educación N° 277 de 2013.

Además, en materia de propiedad intelectual la Ley General de Telecomunicaciones, ley 18.168, establece en su artículo 36 B.- que comete delito de acción pública quien "*sin la autorización del distribuidor legal, comercialice o distribuya una señal de servicios limitados de televisión adecuadamente protegida, o quien, de igual forma, importe, distribuya o comercialice dispositivos tangibles o intangibles destinados a la decodificación de tales señales (…). El que con ánimo de lucro preste servicios de instalación de los dispositivos señalados en el inciso anterior será sancionado (…)*". De esta forma se extiende la protección a las señales de servicios en vivo, que podría aplicarse a servicios de *streaming* por internet.

b.- Aspectos procesales

En este punto analizaremos las herramientas y mecanismos de persecución no intrusivas por parte de las policías y del Ministerio Público además de la presentación en juicio de la prueba proveniente de medios digitales, mientras que las medidas intrusivas serán tratadas en el capítulo 3 con especial atención a la conservación de datos y utilización de agentes encubiertos.

a) Mecanismos de persecución del cibercrimen de las policías y el Ministerio Público.

El Código Procesal Penal no tiene una regulación específica sobre actuaciones en el campo de las redes tecnológicas e informáticas, ni tampoco ha recibido mayores modificaciones a propósito de la ciberdelincuencia, por lo que en principio se aplica la normativa general sobre diligencias de investigación. La compilación y tratamiento de estas medidas supera ampliamente el foco del presente trabajo, sin embargo, trataremos aquí aquellas primeras diligencias de relevancia en el ámbito de la ciberdelincuencia; dejando para el Capítulo 3 lo que se refiere a las medidas intrusivas de interés.

Aquellas diligencias que pueden llevar a cabo las policías sin orden previa; del artículo 83 y 85 del Código Procesal Penal, no presentan alguna particularidad normativa frente al cibercrimen. En general, los delitos de ciberdelincuencia no dan lugar a las hipótesis en que se requiere o justifica la intervención directa e inmediata de la policía, dada su complejidad y mediación de dispositivos tecnológicos que dificultan una rápida denuncia y reacción. Sin embargo, el Ministerio Público ha dado instrucciones generales a las policías para reaccionar frente a delitos en que haya uso de cuenta corriente o celulares, señalando: "*f. En todos aquellos delitos que se encuentren vinculados a un teléfono móvil, computador, tablet u otro dispositivo que utilice simcard, se deberá recabar por escrito la autorización del dueño o titular para acceder al tráfico telefónico e informe de las antenas celulares a las que se ha conectado. En caso de que no se otorgue dicha autorización, comunicarse con el Fiscal a fin de que éste determine la necesidad de solicitar la autorización judicial respectiva.*

g*. En los delitos en que haya uso de cuentas corrientes o tarjetas de crédito, se deberá recabar la autorización escrita del titular para que el banco o entidad financiera respectiva entregue la información protegida por el secreto bancario*."[61]

Estas instrucciones buscan obtener el permiso de la víctima para el acceso a información que corresponde a datos personales, datos que de otra forma no se podría alcanzar legítimamente sin autorización judicial y que podrían resultar esenciales en el esclarecimiento de los hechos. Otra herramienta relevante en ciberdelincuencia es la asistencia internacional que ejecuta la UCIEX a autoridades centrales de otros Estados o a organizaciones internacionales como Interpol, que permite obtener información sobre el ilícito en aquellos casos de comisión transfronteriza, además de las otras diligencias que se soliciten mediante esta vía.

Finalmente, debemos señalar la relevancia de la incautación de objetos de carácter electrónico como una de las primeras medidas en caso de flagrancia, que según lo dispuesto por el artículo 129 del Código Procesal Penal procede sin autorización judicial en el marco del ingreso a lugar

[61] MINISTERIO PÚBLICO. Primeras Diligencias, Instrucciones Generales. Septiembre de 2017. 9 p. [en línea] <http://www.fiscaliadechile.cl/Fiscalia/archivo?id=31695&pid=211&tid=1&d=1> [consulta: 1 de junio de 2020].

cerrado que habilita la norma señalada. Cuando no exista persecución en caso de flagrancia se deberá contar con autorización judicial según lo dispuesto por el artículo 9 y 217, sin perjuicio de la posibilidad de los imputados para entregar voluntariamente sus dispositivos electrónicos.

b) Incorporación en juicio de la prueba proveniente de medios tecnológicos.

Un elemento que es fundamental en el proceso penal es el acceso legítimo a los medios de prueba que serán rendidos en juicio, para lo cual se cuenta con las normas de regulación de diligencias que describen la manera adecuada de acceder a la evidencia, para así cumplir su objetivo respetando los derechos fundamentales de los intervinientes.

Además, para que la prueba cumpla su objetivo de acreditar hechos determinados en juicio, debe ser incorporada al proceso penal en la oportunidad y forma dispuesta por la ley, según lo dispone el Código Procesal Penal, que carece sin embargo de un tratamiento sistemático de la prueba obtenida mediante medios electrónicos.

En el derecho procesal penal chileno rige el principio de **libertad de prueba**, establecido expresamente en el artículo 295 del Código Procesal Penal que establece lo siguiente: "*Todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser probados por cualquier medio producido e incorporado en conformidad a la ley*."[62] Lo aquí dispuesto permite la procedencia de medios digitales de prueba como cualquier otro, siempre y cuando se cumpla con los requisitos legales respecto a la oportunidad y procedencia en su incorporación al juicio.

Luego, el artículo 323 del Código Procesal Penal del párrafo 7° "*Otros medios de prueba*" establece el **principio de analogía**, según el cual el tribunal determinará la forma de incorporación de los otros medios de prueba al procedimiento, adecuándola, en lo posible, al

[62] Libertad que no es absoluta, encontrando limitaciones en la obtención de prueba con infracción de derechos fundamentales; provenientes de diligencias declaradas nulas; registros que intentan sustituir la declaración personal de peritos y testigos; registros de diligencias realizadas por el Ministerio Público o las policías; antecedentes de salidas alternativas o de procedimiento abreviado.

medio de prueba más análogo. En lo que compete al presente trabajo, el Convenio de Budapest en su artículo 14 N°2 letra c) establece que salvo lo dispuesto por el artículo 21 (interceptación de datos relativos al contenido), cada parte aplicará los poderes y procedimientos contemplados en la Sección 2 del Convenio (aquellas referidas a Derecho Procesal) mediante medidas legislativas y de otro tipo para la obtención de pruebas electrónicas de cualquier delito.

El Convenio se centra en las medidas para la obtención de la evidencia, pero no establece disposiciones especiales para la inclusión de la prueba en juicio, de su valoración o procedencia. En nuestro proyecto de adecuación del Convenio tampoco existen elementos al respecto, por lo que no habría modificación a las reglas generales y de actual aplicación.

Un elemento determinante en el control judicial de la prueba incorporada al juicio es la cadena de custodia, lo que se puede volver difuso en la prueba de medios digitales, debido a la vulnerabilidad de la información contenida en soportes electrónicos. Para estos efectos, el proyecto de ley de adecuación del Convenio de Budapest dispone en su artículo 13 una disposición especial según la cual los antecedentes de investigación que se encuentren en formato electrónico serán tratados en su custodia de acuerdo con instrucciones generales que dicte el Fiscal Nacional. De esta forma se deriva el protocolo de custodia al ente persecutor, lo que será esencial para efectos de garantizar que no ocurra vulneración alguna y que debería ser exigido de forma restringida por parte de nuestros tribunales, más allá de su control específico en cada procedimiento judicial.

Con lo dispuesto por el Convenio de Budapest se tiene la ventaja de eventual acceso al registro de todo el tráfico informático en un plazo determinado (actualmente no inferior a un año), en custodia de los proveedores de internet que ante solicitud pasada por Juzgado de Garantía deberán traspasar la información relevante. Si bien esto genera una serie de discusiones respecto al procedimiento y al respeto del principio de proporcionalidad y riesgos asociados de vulneración del derecho a la vida privada, su utilización apropiada será fundamental para actualizar la forma en que se accede a esta evidencia y se acompaña en juicio, toda vez que la

acreditación de la correcta ejecución de la medida y la remisión del ente proveedor de servicios debería ser suficiente acreditación de autenticidad.

En la valoración respecto a la prueba proveniente de diligencias especiales sobre medios electrónicos será fundamental la posición que al respecto tomen los Juzgados de Garantía. Esperamos que se aplique el más estricto estándar de control para efectos de incorporar esta información al juicio, debiendo exigir el cumplimiento de medidas certificadas para asegurar el respeto a los derechos de los intervinientes y la acreditación de una efectiva cadena de custodia mediante el seguimiento de instrucciones objetivas que permitan tener un proceder controlado y seguro.

Respecto de los medios de prueba expresamente regulados por nuestro Código Procesal Penal, en sus artículos 298 y siguientes, lo dispuesto sobre la prueba documental e informe de peritos es esencial al momento de incorporar la prueba proveniente de medios electrónicos. Esta prueba necesariamente debe pasar por un proceso técnico de "traducción" a un medio legible, toda vez que en esencia constituye un código informático transmitido por dispositivos electrónicos el cual debe ser convertido para la comprensión humana. Por tanto, la prueba a rendir será el fruto de este proceso de conversión cuyo resultado generalmente será un documento, una imagen, un video o un registro de audio. Respecto del documento se seguirán las reglas dispuestas por el artículo 333 del Código Procesal Penal. Esta misma disposición establece que cualquier elemento de carácter electrónico se reproducirá en la audiencia de juicio mediante cualquier medio idóneo para su percepción por los asistentes, lo que cubre cualquiera de los resultados señalados y que es la regla general respecto de los llamados modernos medios de prueba.

Cabe destacar que en aquellos casos de extracción compleja de información sobre medios electrónicos procedería el informe de peritos para efectos de acreditar que aquello que se reproduce obedece efectivamente a la información original contenida en el soporte correspondiente. La aplicación de este informe se ajustaría a lo dispuesto por el artículo 314 del Código Procesal Penal al ser necesario la acreditación de los conocimientos técnicos

especiales que requiere tal operación de forma segura como también su conservación e integridad.

2.- Etapa de implementación del Convenio de Budapest

a.- Discusión legislativa[63]

En la tramitación de la aprobación del Convenio, se tuvo presente que el Convenio no es una norma autoejecutable y se requiere de la adecuación de su contenido al derecho nacional. De este modo, la tramitación se centró en los pilares de la problemática de cibercrimen en Chile y la forma en que el Convenio aporta a la persecución del delito cometido a través o con ocasión de medios digitales.

En la discusión en general del proyecto, el Ministro de Relaciones Exteriores subrogante, don Edgardo Riveros señaló que "el principal objetivo del Convenio es el desarrollo de una política criminal común frente al ciberdelito mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional." Reiteró así los pilares principales según los cuales se elaboró el Convenio en el seno del Consejo de Europa y por los cuales se procedió a adherir al mismo.

Además, el Secretario Ejecutivo del Comité Interministerial de Ciberseguridad, Daniel Álvarez, agregó que se conformó un Comité integrado por ocho ministerios más la Agencia Nacional de Inteligencia para el estudio de la aprobación del Convenio enmarcado dentro de la agenda de ciberseguridad nacional. Añadió su interés por la pronta aprobación, atendiendo a la globalidad de los fenómenos delictivos por medios informáticos. Señaló que "*En Chile, el delito informático más recurrente es la clonación de tarjetas, lo cual también es un ciberdelito internacional, porque hay transferencias de las bases de datos de las tarjetas transfronterizas, o sea, se clonan en Chile, pero se empiezan a ocupar fuera del país, en un par de horas*".

[63] BIBLIOTECA del Congreso Nacional. Historia del Decreto N° 83 que promulga el Convenio sobre la Ciberdelincuencia. [en línea] <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6527/> [consulta: 1 de junio de 2020]

Por otra parte, personal de la Policía de Investigaciones (PDI) remarcó la utilidad que significaría la actualización de la regulación en materia de ciberdelincuencia en los tipos penales más recurrentes en nuestro país, abuso sexual, clonación y fraude; señalando la dificultad de dar con los responsables de la clonación de tarjetas, toda vez que se realiza mediante una operación disgregada en sus etapas, en el territorio nacional y en el extranjero.

Representando a la sociedad civil, concurrió la ONG Derechos Digitales, expresando su acuerdo con la necesidad en actualizar la regulación y por tanto adherir al tratado, pero debiendo realizarse de forma cuidadosa con los derechos de los ciudadanos, en particular en lo que se refiere al registro, confiscación y obtención en tiempo real de datos, lo que debería aprobarse con las flexibilidades necesarias manteniendo el debido proceso.

Finalmente; en el Congreso, existió consenso en la necesidad de adoptar el Convenio y actualizar la normativa nacional para reforzar la persecución de los delitos informáticos. Además, se manifestó preocupación por la ciberseguridad en tiempos de que el sabotaje informático se ha convertido en una de las principales herramientas de ataque contra la seguridad interior de las naciones, por lo que se hace urgente modernizar la regulación existente y propender a mayor colaboración internacional.

En consideración a lo expuesto, y al apoyo unánime expresado por las instituciones vinculadas y por las distintas fuerzas políticas del Poder Legislativo, el día 16 de noviembre del año 2016 se aprobó la adhesión al Convenio de Budapest en el Senado con las declaraciones y reservas presentadas por el Ejecutivo, sin modificación alguna.

El día 25 de octubre de 2018, mediante boletín N°12192-25 se ingresaría al Senado el proyecto de ley que “establece nomas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest”, lo que abriría el paso a la discusión pormenorizada de las disposiciones del Convenio y su adecuación a la normativa nacional, temas a tratar en el título IV del presente estudio.

b.- Ratificación

Dentro del proceso de invitaciones a adherirse al Convenio para países que no pertenecen a la Unión Europea, el Comité de Ministros del Consejo de Europa invitó a Chile a formar parte del Convenio el día 18 de junio del 2009. Con anterioridad nuestro país a través de Cancillería ya habría analizado, desde el año 2004, la posibilidad y conveniencia de adherir al Convenio, sin lograr mayor avance en la tramitación interna. En agosto de 2009, el Ministerio del Interior, mediante decreto N°3265 creó al efecto una comisión interministerial para su estudio, que llevó a la elaboración del proyecto de ley.

En noviembre de 2010 la Cámara de Diputados mediante su Sesión 101 presentó al ejecutivo su proyecto de acuerdo N°231, mediante el cual comunica: "(…) *de conformidad a las competencias que le asigna el artículo 32 número 15 de la Constitución Política de la República, se exhorta a S.E. el Presidente de la República, para que tome las medidas tendientes a que nuestro país adhiera formalmente al Convenio de Budapest, principalmente en lo referente a la puesta en funcionamiento de la comisión interministerial constituida para tal efecto.*"

El Ejecutivo ingresó al Congreso el proyecto de ley que aprueba el "Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001" el 16 de mayo de 2016, sin urgencia. Según lo dispuesto por nuestra Constitución en sus artículos 54 N°1) y 66 inciso cuarto, su aprobación requería quorum simple, logrando ser adoptado por unanimidad en la Cámara de Diputados en su primer trámite constitucional con fecha 11 de agosto de 2016, dando razón a la evidente necesidad de tener este tipo de regulación para la protección de los derechos en el ciberespacio, como también para la protección de la nación en el marco de la agenda de ciberseguridad y de colaboración entre instituciones a nivel internacional para este objetivo. Finalmente, se promulgó el Convenio mediante el Decreto N°83 del Ministerio de Relaciones exteriores el 27 de abril de 2017.

c.- Roles y funciones

a) *Asistencia Mutua y Autoridad Central*

Uno de los pilares del Convenio es la coordinación internacional para efectos de conseguir la persecución eficaz de los delitos informáticos que en muchas ocasiones traspasan las fronteras de jurisdicción nacional. Actualmente existe una multiplicidad de Convenios de asistencia mutua en materia penal, tanto de carácter bilateral como multilateral[64], en los que establece el concepto de autoridad central como institución clave en la tramitación efectiva de solicitudes en esta materia. Así, la idea es que el Estado requirente y el Estado requerido de la solicitud se comuniquen a través de una autoridad especializada determinada por cada Estado, que no obedezca a la coyuntura diplomática y permita mayor celeridad que la vía judicial que procedería en términos generales.

Dentro de la tramitación del Convenio se evaluó el establecimiento de un régimen distinto, con carácter general y que sustituyera la regulación existente a la fecha en la materia. Sin embargo, se rechazó esta idea y se decidió mantener la lógica vigente establecida en distintos tratados en relación a la asistencia internacional, la autoridad central y los procedimientos de solicitudes. Estableciéndose, por tanto, un sistema supletorio ante la carencia de una regulación particular entre las Partes al momento de realizar la solicitud, siguiendo los mismos lineamientos establecidos en materia internacional, es decir la comunicación entre autoridades centrales encargadas de la tramitación de las solicitudes de asistencia mutua, siempre y cuando no exista un tratado o acuerdo entre las partes.

b) Ministerio Público como Autoridad Central.

Tal como fue planteado en el título 4 del Capítulo I, el rol que tiene la autoridad central en la asistencia internacional es muy importante, en específico, en el marco del Convenio de Budapest, debe estar a cargo de la ejecución y celeridad de las solicitudes de asistencia.

Al momento del depósito del instrumento de adhesión al Convenio, la República de Chile designó como autoridad central y punto de contacto de la Red 24/7 al Ministerio Público de

[64] Tales como la Convención Europea de Asistencia Mutua en Materia Penal, suscrita en Estrasburgo, el 20 de abril de 1959 y complementada por sus protocolos adicionales.

Chile como ha sido la tónica en materia de Convenios de asistencia mutua en materia penal[65]. Previamente todos los requerimientos de asistencia internacional pasaban de forma obligatoria por la Dirección de Asuntos Jurídicos de la Cancillería, hasta que en diciembre de 2017 el Canciller (s) don Edgardo Riveros firmó junto al Fiscal Nacional don Jorge Abbot el traspaso de funciones, cuya vigencia comenzó a aplicar con fecha 1 de febrero de 2018. Así, el Ministerio Público comenzó a tramitar las solicitudes internacionales de forma directa con las autoridades centrales de los otros Estados con los cuales se tenga una relación de asistencia mutua en materia penal, cumpliendo, por tanto, con el objetivo de contacto directo y celeridad en el trato de requerimientos internacionales que tanta prioridad ha tenido en diversos tratados internacionales. Esta función recae en particular en la UCIEX.

Este rol no es una novedad del Convenio de Budapest; de hecho, el Ministerio Público es la Autoridad Central en varias convenciones internacionales, en particular las siguientes: "*1.- Convención Interamericana sobre Asistencia Mutua en Materia Penal, adoptada en Nassau el 23 de mayo de 1992 y su Protocolo Facultativo, suscrito en Managua el 11 de junio de 1993. Artículo 3 de la Convención; 2.- Acuerdo de Asistencia Jurídica Mutua en Asuntos Penales entre los Estados Parte del MERCOSUR y la República de Bolivia y la República de Chile, adoptado en Buenos Aires el 18 de febrero de 2002. Artículo 3 de la Convención; 3.- Convención Europea de Asistencia Mutua en Materia Penal, adoptada en Estrasburgo el 20 de abril de 1959; su Protocolo Adicional de 17 de marzo de 1978; y su Segundo Protocolo Adicional de 8 de noviembre de 2001. Artículo 15 párrafo 6° de la Convención; y Artículo 4 párrafo 8, letra d) del Segundo Protocolo Adicional; 4.- Convención Interamericana contra la Corrupción, adoptada en Caracas el 29 de marzo de 1996. Artículo XVII de la Convención; 5.- Convención Interamericana contra la Fabricación y el Tráfico de Ilícitos de Armas de Fuego, Municiones, Explosivos y otros Materiales Relacionados, adoptada en Washington D.C. el 14 de noviembre de 1997. Artículo XVII N°2 de la Convención; 6- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, adoptada en Palermo el 15 de noviembre de 2000 y*

[65] A excepción de la extradición, en cuyo caso, la autoridad central continúa siendo la Dirección de Asuntos Jurídicos del Ministerio de Relaciones Exteriores.

sus Protocolos. Artículo 18 N°13 de la Convención; 7.- Convención de las Naciones Unidas contra la Corrupción, adoptada en Nueva York el 31 de octubre de 2003. Artículo 46 N°13 de la Convención; 8.- Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas, adoptada en Viena el 20 de diciembre de 1988. Artículo 7 N°8 de la Convención; 9.- Convención para Combatir el Cohecho a Funcionarios Públicos Extranjeros sobre la Ciberdelincuencia, adoptada en Budapest el 23 de noviembre de 2001. Artículos 27 N°2 y 35 de la Convención; otros Tratados bilaterales como el Tratado de Extradición y Asistencia Judicial en Materia Penal entre la República de Chile y el Reino de España, suscrito en Santiago el 14 de abril de 1992."[66]

La determinación del Ministerio Público como autoridad central, y el trabajo de la UCIEX en específico permite una dedicación especializada en el tratamiento de los requerimientos internacionales (pasivos y activos), dotando de mayor eficacia y eficiencia a la persecución penal, a través de diversos vínculos de trabajo internacional.

3.- Declaraciones y reservas efectuadas al Convenio

a.- Declaraciones

En conformidad a lo dispuesto por el propio Convenio en su artículo 40; y con el objetivo de exigir mayores requisitos a los que establece este instrumento, el Ejecutivo decidió realizar las siguientes declaraciones[67]: 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 Ley N°19.223 sobre delitos informáticos*". b.) "*La República de Chile declara que exigirá un ánimo fraudulento que*

[66] SEGOVIA Arancibia, Antonio. Los equipos conjuntos de investigación como herramienta de Cooperación Internacional. Revista Jurídica del Ministerio Público N ° 72- abril 2018. pp 75-76.

[67] "Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e)."

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".

Estas declaraciones corresponderían a las primeras adecuaciones que se proponen a la adopción del Convenio con el objetivo de armonizar su contenido con la normativa nacional del Código Penal, Código Procesal Penal y la Ley N°19.223. Ambas declaraciones apuntan al elemento subjetivo en la comisión del hecho punible, y que tiene por finalidad excluir un conjunto de conductas que, si bien se podrían enmarcar en los tipos contemplados por el Convenio, no tienen una finalidad delictiva sino preventiva o de uso legítimo de la red. Se podría afirmar que el uso de buena fe se encontraría de todos modos permitido, dado que no se cumpliría con uno de los requisitos indispensables de la responsabilidad penal: la culpa o dolo. Sin embargo, el incluir este requisito dentro del tipo penal obedece a una técnica legislativa que trae más claridad respecto de lo que objetivamente se encuentra penado, manteniendo de todas formas la complejidad de su determinación.

b.- Reservas

Respecto a las reservas, el Convenio contempla de manera expresa en su artículo 42[68] la posibilidad de incorporar reservas a las disposiciones del mismo, como, por ejemplo, al artículo 4 sobre ataques a la integridad de datos, al artículo 6 sobre abuso de los dispositivos, al artículo 9 sobre delitos relacionados con la pornografía infantil, al artículo 20 sobre obtención en tiempo real de datos obtenidos de tráfico, entre otras. Estas reservas se permiten de plano en la adhesión del Convenio, pero están limitadas en su forma y contenido a lo dispuesto por el mismo Convenio. Así; por ejemplo, la reserva realizada respecto al artículo 11 sobre tentativa y complicidad puede recaer solamente en el párrafo segundo referente a la tipificación como delito de la tentativa deliberada en la comisión de los delitos contemplados por el Convenio,

[68] "Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva".

no así sobre el párrafo primero respecto a la tipificación como delito de la complicidad deliberada. Cualquier otro tipo de reserva se encuentra prohibida según el artículo 42 del Convenio.

El ejecutivo presentó el proyecto de aprobación del Convenio con las siguientes reservas: a) "*La República de Chile expresa, de conformidad al Artículo 4, párrafo 2, del Convenio sobre la Ciberdelincuencia, que tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".* b) "*La República de Chile expresa, de conformidad al Artículo 6, párrafo 3 del Convenio sobre la Ciberdelincuencia, que no aplicará el párrafo 1 del mismo Artículo, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado Artículo 6*". c) "*La República de Chile expresa, de conformidad al Artículo 9, párrafo 4, del Convenio sobre la Ciberdelincuencia, que no aplicará los apartados b) y c) del párrafo 2 del mismo Artículo*". d) "*La República de Chile expresa, de conformidad al Artículo 22, párrafo 2, del Convenio sobre la Ciberdelincuencia, que no aplicará las normas sobre jurisdicción establecidas en el apartado 1 d. del mismo Artículo*". e) "*La República de Chile se reserva, en relación con el Artículo 29, párrafo 4, del Convenio sobre la Ciberdelincuencia, el derecho a denegar la solicitud de asistencia internacional en caso de que la conducta perseguida no esté tipificada en Chile al momento del requerimiento*".

Tanto las declaraciones como las reservas presentadas por el Ejecutivo serían ratificadas por el Congreso de forma íntegra. Sus efectos serán parte del siguiente título a propósito del proyecto de Ley de adecuación del Convenio.

4.- Proyecto de Ley de adecuación

A la fecha, existe un proyecto de ley ingresado al Senado mediante boletín N°12192-25[69] que "*establece nomas sobre delitos informáticos, deroga la ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest*", que data del 25 de octubre del 2018. Este proyecto ya fue aprobado por la Cámara de origen; con fecha 3 de marzo de 2020, y a la fecha de término de este trabajo se encuentra actualmente en su segundo trámite constitucional ante la Cámara de Diputados[70].

En su Mensaje el ejecutivo describe el contexto actual respecto al uso consolidado de las redes y remarca la relevancia de adoptar una nueva normativa nacional que contemple un contenido procesal, a diferencia de la ley 19.223 de 1993, la cual ha quedado evidentemente sobrepasada ante el avance de la tecnología y su masificación. Se señala, además, que constituye un pilar de la Política Nacional de Ciberseguridad 2017-2022 aprobada por nuestro país como política de Estado.

Luego en la Comisión de Seguridad Pública, se dio paso a la discusión general del proyecto, con intervenciones de autoridades y miembros de la sociedad civil, donde se terminó aprobando en general la idea de legislar el 13 de marzo de 2019. En sesión ordinaria N° 106 de 3 de marzo de 2020 se aprobó en particular el proyecto, pasando a la Cámara de Diputados para el segundo trámite constitucional con una serie de modificaciones aprobadas al texto original.

El proyecto de ley presentado por el ejecutivo consta de 17 artículos y 3 disposiciones transitorias, estableciendo normas de derecho penal sustantivo a través de un catálogo de delitos, agravantes y atenuantes particulares, optando así por el establecimiento de un sistema regulatorio propio fuera del Código Penal. Desde ya esta opción nos parece poco conveniente

[69]SENADO DE LA REPÚBLICA. Boletín 12.192-25. 2018 [En línea] <https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=12192-25> [consulta: 22.05.2020]

[70] CÁMARA DE DIPUTADAS Y DIPUTADOS. Proyecto de Ley: Establece normas sobre delitos informáticos, deroga la Ley N°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest. [En línea] <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12715&prmBOLETIN=12192-25> [consulta: 01.06.2020]

toda vez que se contribuye a la atomización de la ley penal mediante leyes especiales que se condice con un alejamiento de los principios de nuestra normativa rectora en la materia, como se evidenciaría en el mismo proyecto de ley que olvida siquiera referenciar cuáles serían los bienes jurídicos protegidos por los nuevos tipos. Lo regulado constituyen materias que por su relevancia y generalidad deberían formar parte del Código Penal no sólo por motivos académicos, sino que también por motivos sistemáticos y hermenéuticos en la aplicación de la norma.

Además, el proyecto establece un título sobre normas de carácter procesal como lo son disposiciones de competencia, atribuciones de investigación del Ministerio Público; entre otras. Adicionalmente, se establecen disposiciones finales en las que se encuentran definiciones, derogación de la ley 19.223, y modificaciones al Código Procesal Penal donde se encuentran algunas de las materias más discutidas por su afectación a los derechos fundamentales.

Título I "De los delitos informáticos y sus sanciones"

En materia penal sustantiva, el proyecto establece las siguientes figuras:

1- Perturbación informática.[71] Se establece un tipo penal nuevo, que no estaba contemplado en el Convenio de Budapest. Así planteado parece tomar el lugar del ataque a la integridad del sistema, del artículo 5 de tal instrumento, correspondiente a lo que conocemos como "*hacking*", sin embargo, se establece de manera demasiado amplia y no incorpora los requerimientos del Convenio en relación a que la conducta debe constituir una obstaculización grave, deliberada e ilegítima. Otro elemento que suscitó críticas fundadas fue la configuración del elemento subjetivo del tipo "*maliciosamente*" que implica dolo directo y proviene de la ley 19.223, en lugar de utilizar los parámetros del Convenio de Budapest que son más claros. En

[71] "El que maliciosamente obstaculice o perturbe el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será castigado con la pena de presidio menor en su grado medio a máximo. Si además se hiciere imposible la recuperación del sistema informático en todo o en parte, se aplicará la pena de presidio menor en su grado máximo."

el texto que hoy se discute se ha corregido, y se trata como delito de "*ataque a la integridad de un sistema informático*", luego de que la Comisión de Seguridad Pública en primer trámite constitucional acordara adoptar la nomenclatura del Convenio, además se modificó "*maliciosamente*" por "*deliberada e ilegítimamente*". Adicionalmente se prevé que el obstáculo debe ser grave.

2- Acceso ilícito.[72] Esta disposición contiene 3 supuestos: un tipo penal base, un supuesto agravado por el objetivo lesivo de la conducta en su inciso segundo y una hipótesis calificada por la circunstancia de penetrar o evadir medidas de seguridad en su inciso tercero.

Respecto de la figura agravada y de la calificada, nos parece que son muy amplias en consideración a la figura base. Esto porque se agrega; primero, la intención de apoderarse, usar o incluso *conocer* la información, lo que sería extensible a casi todos los casos concebibles.

Luego, la figura calificada es a su vez bastante amplia ya que se establece la evasión o vulneración a las medidas de seguridad para impedir el acceso; lo que también sería aplicable a la generalidad de los casos, toda vez que los sistemas digitales cuentan con medidas de distinta índole para la protección de su información y es difícil concebir un acceso indebido sin encontrar barrera alguna[73] (sería información abierta o de acceso público, por lo que no habría delito).

3- Interceptación ilícita.[74] Esta es una figura que sigue lo determinado por el Convenio de Budapest en su artículo 3° pero incluye dos particularidades: la exigencia de un actuar malicioso y una figura calificada para los casos de interceptación de emisiones

[72] "El que indebidamente acceda a un sistema informático (…)"
"El que indebidamente acceda con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático (…)"
"Si en la comisión de las conductas descritas en este artículo se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas para impedir dicho acceso (…)"

[73] Observación aportada por el encargado de Políticas Públicas de Derechos Digitales América Latina, don Pablo Violler en las sesiones de la Comisión de Seguridad en primer trámite constitucional.

[74] "El que indebida y maliciosamente intercepte o interfiera la transmisión no pública de información entre los sistemas informáticos (…).
El que capte ilícitamente datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas de los dispositivos (…)."

electromagnéticas de los dispositivos. Respecto del componente subjetivo de conducta maliciosa, corresponde a un elemento residual de la ley 19.223 y como hemos señalado previamente, produce complejidades elevadas en su acreditación a diferencia de los parámetros del Convenio.

Luego, llama la atención que la figura calificada no exige la conducta maliciosa, sólo una conducta ilícita. Además, establece una penalidad mayor por interceptar la información a través de un medio en particular: las emisiones electromagnéticas. Debemos entender este tipo de interceptación como aquella que corresponde a la operación de ondas electromagnéticas de baja o alta frecuencia dentro del espectro electromagnético, que son utilizadas por la telefonía celular y redes de conexión inalámbrica a internet.

Sin existir referencia alguna en la historia legislativa del proyecto a la fecha, podríamos entender que la interceptación de las comunicaciones entre aparatos de telefonía móvil mediante llamadas o aplicaciones de mensajería no requeriría el elemento subjetivo y tendría una sanción mayor en consideración a la gravedad de afección sobre el derecho a la privacidad y la seguridad en las comunicaciones privadas establecido en nuestra Constitución en su artículo 19 N°4 y N°5, toda vez que este tipo de comunicación constituyen una parte esencial de la vida de todo ciudadano en las sociedades contemporáneas y la presunción de su inviolabilidad un pilar fundamental del funcionamiento comunitario.

Finalmente, surge la duda respecto a si en el ejercicio de las facultades persecutoras, los agentes del Ministerio Público y de las policías podrían incurrir en esta figura al realizar interceptaciones de mensajería electrónica sin la autorización judicial correspondiente; produciendo ya no solo una prueba ilícita, sino también un delito. En este sentido, efectivamente cada dispositivo móvil podría considerarse como “un sistema informático” según las definiciones del Convenio y podría acreditarse la figura siempre y cuando se cumpla con el requisito de constituir un acto “ilícito”, es decir completamente alejado de las facultades legales correspondientes y sus requisitos de procedencia. Nos parece así, del todo lógico que

en casos de abuso deliberado de herramientas de interceptación fuera de todo margen legal, corresponda aplicar esta figura.

4- Daño informático.[75] Esta figura obedece a la adaptación del artículo 4° del Convenio de Budapest caratulado como "ataque a la integridad de los datos", el que desde ya pareciera más adecuado y preciso para la conducta punible. Se incluye en el proyecto lo señalado en la reserva hecha por nuestro país en la suscripción del Convenio en relación a la exigencia de daño grave como efecto de la conducta ("daño serio" en el proyecto).

La inclusión del estándar de conducta maliciosa en este artículo pareciera improcedente con el compromiso internacional de nuestro país. Esto porque el Convenio de Budapest plantea una reserva expresa; utilizada por Chile, pero solo respecto de la exigencia de daños graves, no de la "intención delictiva" como sí lo señala en otras disposiciones ya analizadas. Además, Chile declaró la inclusión del criterio subjetivo de la ley 19.223 en los delitos tipificados en los artículos 2 y 3 del Convenio de Budapest, siendo que el ataque a la integridad de los datos o daño informático está en el artículo 4, por lo que se produce una clara contradicción con el instrumento internacional y eventuales entorpecimientos en la persecución penal y colaboración internacional. Actualmente se trata del delito de "ataque a la integridad de los datos informáticos" luego de que la Comisión de Seguridad Pública en primer trámite constitucional decidiera adoptar la nomenclatura del Convenio, además en la tramitación se agregó que el daño sea producido ilegítimamente, siguiendo las recomendaciones de la Corte Suprema para evitar que incurra en este delito un administrador habilitado para eliminar o alterar datos.

5- Falsificación informática.[76] Las figuras aquí establecidas es una adaptación bastante fiel del artículo 7 del Convenio de Budapest y busca aplicar el reproche de lo dispuesto en las

[75] "El que maliciosamente altere, borre o destruya datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño serio al titular de los mismos."
[76] "El que maliciosamente introduzca, altere, borre, deteriore, dañe, destruya o suprima datos informáticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, será sancionado con las penas previstas en el artículo 197 del Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público, caso en que se sancionará con las penas previstas en el artículo 193 de dicho cuerpo legal."

disposiciones que tipifican los delitos de falsificación de documento público o auténtico cometido por funcionarios públicos en el caso del artículo 193 del Código Penal y de falsificación de documento privado con perjuicio a tercero en el artículo 197 del mismo cuerpo. Si bien en materia de prueba en juicio corre la regla general de medios análogos respecto de lo que a documentos se refiere, cuando tratamos la normativa penal el hecho de que la falsificación de datos no se encuentre incorporada expresamente en el tipo deja fuera todos aquellos casos de manipulación fraudulenta de información digital que no se considere como documento para los efectos legales mediante una interpretación restrictiva. En este sentido nos parece un aporte oportuno a la legislación penal.

6- Fraude informático.[77] La figura aquí transcrita es una adaptación del artículo 8 del Convenio de Budapest, pero prescinde del requisito del Convenio sobre el acto "deliberado e ilegítimo" incorporando la finalidad de obtener beneficio económico ilícito para sí o para un tercero, causando daño a otro. Esta modificación nos parece bastante acertada toda vez que si bien constituye un elemento subjetivo (la finalidad), tiene parámetros más claros en su determinación y evita que la mera utilización de la información de un sistema informático sea punible.

Un elemento interesante para analizar respecto de este delito es cómo se posiciona con lo dispuesto por la ley 20.009 que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas.

Finalmente, en la Comisión de Seguridad Pública del Senado tanto la Policía de Investigaciones como la Asociación de Bancos e Instituciones Financieras pidieron incorporar a esta figura el receptador de los fondos, incluso sin el conocimiento del ilícito; dado que muchas veces se le encuentra con mayor facilidad que al perpetrador directo. Esto nos parece excesivo y peligroso respecto de sus contornos. No corresponde aplicar esta figura a quien meramente presta su

[77] "El que, causando perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, utilice la información contenida en un sistema informático o se aproveche de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático (…)."

cuenta para el depósito de fondos sin el conocimiento de su origen, además en caso de que tenga conocimiento ya existen mecanismos para perseguir su responsabilidad penal.

7- Abuso de los dispositivos.[78] Esta figura proviene de lo dispuesto por el artículo 6 del Convenio de Budapest. El objetivo es obstaculizar el desarrollo, utilización y comercialización de dispositivos físicos o digitales que tienen por fin la comisión de delitos aquí tipificados. La adaptación del proyecto traduce el requisito de "intención delictiva", donde los dispositivos y demás elementos operan como un medio y ejemplifica de buena forma las herramientas generalmente utilizadas en la comisión de delitos informáticos. Donde el proyecto no se extiende es a los medios comisivos que sí contiene el proyecto como la posesión o la fabricación de este tipo de dispositivos, lo que en teoría permitiría su elaboración y tenencia, debiendo probar la utilización o circulación del elemento.

Debemos hacer extensivo; además, lo señalado previamente respecto a los operadores de ciberseguridad que operan mediante el llamado "*hackeo ético*" que implica la búsqueda de vulnerabilidades en variados sistemas para luego informarlos al titular del sistema. Estas operaciones se realizan precisamente mediante la fabricación y utilización de mecanismos de vulneración para adelantarse a posibles ataques, lo que debería quedar expresamente fuera de la norma para así no crear disuasión alguna a este tipo de operaciones.

Título II "Del procedimiento"

En materia procesal se incorporan varias normas particulares cuyo fin es facilitar la investigación penal de los hechos punibles y la determinación de los responsables en atención a la particularidad de este tipo de delitos. Se establecen así mayores facultades de investigación y normas de manejo de datos en general que han conllevado una amplia

[78] "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 5° 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."

discusión en torno al límite de estas disposiciones y la eventual vulneración de derechos. A continuación, analizaremos estas normas en su contenido y proyección a la luz de lo establecido por el Convenio de Budapest y de los derechos fundamentales que se podrían ver vulnerados en su caso.

1- Legitimidad activa: Las investigaciones podrán iniciarse por el ejecutivo mediante querellas presentadas por el Ministerio del Interior o delegados presidenciales regionales y provinciales cuando las conductas interrumpieren el normal funcionamiento de un servicio de utilidad pública.

Esta disposición tiene por objeto permitirle al ejecutivo promover directamente el inicio de la investigación mediante querella en el caso determinado. Si bien se comprende la relevancia que tiene el normal funcionamiento de los servicios de utilidad pública que se pueden ver seriamente comprometidos por ataques informáticos; no parece necesaria una norma de esta naturaleza toda vez que la investigación penal radica constitucionalmente en el Ministerio Público y el Ejecutivo se debería limitar a denunciar; en caso contrario, se corre el riesgo de utilizar políticamente el procedimiento penal.

2- Facultades investigativas del Ministerio Público: El Convenio ordena a cada Parte adoptar las medidas legislativas y de otro tipo que sean necesarias para facilitar la ejecución de sus medidas a través de las autoridades competentes, mandato que se consagra a través del artículo 14 N°1 en general y en cada medida procesal en particular. Además, el artículo 15 establece que la ejecución de estas medidas en el campo interno "*deberá garantizar una protección adecuada de los derechos humanos y de las libertades*" y en concreto deberá respetar los instrumentos internacionales sobre derechos humanos y el principio de proporcionalidad. Luego, el artículo 15 en su inciso 2° señala que las partes podrán incluir "supervisión judicial" como salvaguarda de las medidas, cuando proceda en consideración del procedimiento, dejando por tanto el campo abierto a la aplicación directa de las medidas sin control judicial según lo considere el Estado. Finalmente, cada una de las medidas mencionadas establece que "*Los poderes y procedimientos mencionados en el presente*

artículo están sujetos a lo dispuesto en los artículos 14 y 15", reiterando la preminencia de los principios conservadores.

El proyecto de ley de adecuación del Convenio de Budapest en Chile de actual tramitación en boletín N°12192-25; establece distintas facultades que clasificaremos en:

1. Técnicas especiales del artículo 11;

2. Regla especial de comiso y;

3. Medidas procesales mediante modificaciones al Código Procesal Penal.

<u>1- Técnicas especiales del artículo 11:</u> Establece distintas facultades investigativas del Ministerio Público en sus dos incisos, siendo las siguientes:

a) La aplicabilidad de lo dispuesto por los artículos 222 a 226 del Código Procesal Penal con relación a la interceptación de comunicaciones telefónicas y a la utilización de otros medios técnicos de investigación y captación de imágenes o video incluyendo la grabación de audio en la comunicación entre presentes sobre los delitos especiales contenidos en el proyecto. A esto se complementa la incorporación de un artículo 222 bis relacionado a la conservación rápida de datos informáticos. Estas técnicas de investigación ya están establecidas respecto a delitos en general, debiendo siempre dar cumplimiento a sus requisitos específicos; lo que haría el proyecto sería entonces incorporarlas de forma expresa. Sin embargo, el artículo 11 restringe su aplicación a casos en que fuera imprescindible y existieren sospechas fundadas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer estos ilícitos, debiendo contar siempre con resolución judicial. De esta forma, nos parece que, si bien se tratan de medidas que conllevan una fuerte vulneración de derechos fundamentales, el establecimiento de los requisitos descritos que se acumulan a los límites del Código Procesal Penal permitiría un uso más restrictivo y siempre bajo el control del juez de garantía.

b) Técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la ley N°20.000. Lo aquí dispuesto sigue la tendencia nacional de ampliar expresamente la aplicación de figuras especiales como el agente encubierto a cada vez más categorías de delitos. Respecto a sus requisitos de procedencia, se debe estar a lo dispuesto por la ley 20.000 y su aplicación especial debe ser necesaria para la investigación penal o la prevención de otro delito. Lo interesante a este respecto es la forma de ejecución de estas técnicas en un contexto de medios digitales, donde el agente encubierto puede operar en las más amplias formas -desde el contacto particularizado a sujetos sospechosos hasta participación en foros amplios de carácter delictivo, con infinidad de herramientas online- y por tanto los límites de su actuar se vuelven aún más complejos.

2- Regla especial de comiso: Establecida en el artículo 12 del proyecto de adecuación, podría afectar la diligencia de incautación de objetos y documentos establecida en el artículo 217 del Código Procesal Penal, toda vez que dentro de los objetos susceptibles de incautación se encuentran aquellos que "pudieran ser objeto de la pena de comiso", por lo que se ampliaría su aplicación por lo dispuesto por el proyecto. En cualquier caso, se requiere de autorización judicial para su incautación (exceptuando la entrega voluntaria), lo que constituye un control adecuado al efecto.

3- Modificaciones al Código Procesal Penal: Analizaremos las modificaciones a propósito de las facultades investigativas, profundizando este apartado del proyecto al trabajar las disposiciones finales.

a) Preservación provisoria de datos informáticos: Contando con autorización judicial dentro de un plazo de 90 días prorrogable una única vez, el Ministerio Público podría acceder a la información por parte de los proveedores. Nos parece que la medida respeta el principio de proporcionalidad y en sí no implica afectación alguna al ser una conservación de información sin acceso en principio, debiendo pasar por autorización judicial fundada para el acceso de tal información.

b) Facilitación de datos o comunicaciones transmitidas o recibidas por proveedores de internet: Esta medida constituye una figura sui géneris a las que contempla el Convenio de Budapest. Sería asimilable a la orden de presentación, pero con un contenido más amplio e indeterminado. Se establece que procede a orden del fiscal con autorización judicial, en un plazo señalado en la misma resolución. Los principales problemas con esta medida se describirán en el análisis pormenorizado del proyecto de ley, pero como diligencia de investigación constituye un riesgo para cualquier usuario del servicio de redes de internet al no estar determinado de forma clara. Esto obedece a una mala técnica legislativa que se alejó de los parámetros del Convenio para dejar en su defecto una figura que; si bien debe pasar por un control judicial a priori, presenta graves riesgos para el contenido esencial del derecho a la privacidad ante la eventual generalidad de información traspasada sin consentimiento y conocimiento del titular de ésta.

Las diligencias descritas se encontrarían en la necesidad de pasar por evaluación y autorización judicial previa para efectos de llevarse a cabo, lo que constituye una correcta barrera para la protección de los derechos fundamentales por parte del Juez de Garantía. Sin embargo, existe el riesgo de que incluso con el control judicial previo se produzcan vulneraciones en la forma concreta de realización de las diligencias, elemento que no se encuentra bien regulado ni siquiera respecto de las diligencias tradicionales de nuestra legislación según el principio de investigación desformalizada. Esto es de especial importancia cuando hablamos de prueba electrónica o digital en consideración a la facilidad de sobrepasar los límites pertinentes en la investigación de hechos determinados, toda vez que en el acceso a información específica se puede traspasar el derecho de privacidad del imputado o incluso de terceros o en esferas que escapan absolutamente de los hechos investigados.

3- Custodia especial de antecedentes en formato electrónico: “Art. 13: Sin perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su

preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el Fiscal Nacional"

Los antecedentes en soporte electrónico pueden ser eliminados de manera más simple y sin dejar evidencia mediante operaciones digitales. Es por esta vulnerabilidad que se establece esta norma que tiende a su mayor protección mediante las instrucciones que al efecto dicte el Fiscal Nacional, dándole así mayor posibilidad al Ministerio Público de cautelar el manejo de este tipo de evidencia más allá de las reglas generales.

Título III "Disposiciones finales"

1- Definiciones: En el artículo 14 del proyecto se replican las definiciones establecidas en el Convenio de Budapest respecto "datos informáticos" y "sistema informático" en su artículo 1.

El problema de esta disposición es, por una parte, su ubicación dentro el proyecto. No se entiende por qué dejar las definiciones en las disposiciones finales y no al comienzo como bien lo hace el Convenio, considerando que son términos que se utilizan reiteradamente a través del cuerpo de la normativa. El otro problema es su insuficiencia, ya que deja fuera 2 definiciones que están en el mismo Convenio que corresponden a "proveedor de servicios" y "datos relevantes al tráfico"; este último concepto estaría incorporado en el artículo 16. Estos últimos términos no tendrían por qué excluirse de este artículo y son conceptos relevantes para la aplicación de normas que no sólo están en el Convenio, sino que también se adaptan al proyecto.[79]

2- Derogación de la ley 19.223: Toda referencia legal a tal norma se entenderá hecha a esta ley.

[79] Es especialmente relevante el concepto de proveedor de servicios por lo ya analizado en el Capítulo I, Título V.

3- Modificaciones al Código Procesal Penal: Bajo esta denominación se encuentran en el proyecto 3 importantes medidas procesales cuyo procedimiento y control procederemos a analizar

a) Se agrega al artículo 218 bis la preservación provisoria de datos informáticos[80]: Esta disposición hace eco de las medidas procesales principales establecidas en la Convención de Budapest en su artículo 16 respecto a la "conservación rápida de datos informáticos", ya analizada previamente. Está suficientemente delimitada como para afirmar que responde a criterios adecuados de proporcionalidad en el cumplimiento de su objetivo.

b) Se reemplaza el artículo 219 del Código Procesal Penal (actualmente suprimido) por una disposición que establece la obligación de los proveedores de internet; o de las concesionarias que operen con ellos, frente a un requerimiento del Ministerio Público aprobado por el Juez de Garantía, la facilitación de datos o comunicaciones transmitidas o recibidas por ellas, exceptuando las telefónicas (que siguen lo dispuesto por el artículo 222 del Código Procesal Penal). Esta entrega de datos o comunicaciones que pasan por la empresa se hará en el plazo que determine la resolución judicial y será de responsabilidad directa de un encargado que tendrán que nombrar estas empresas, so pena de sanciones que pueden llegar incluso al gerente general y representante legal de la empresa mediante arresto en caso de negativa de entrega de la información.

Lo aquí dispuesto pareciera similar a la orden de presentación dispuesta por el artículo 18 del Convenio de Budapest, pero tiene diferencias relevantes; en concreto, la orden de presentación también se dirige a los proveedores de servicios de internet, pero está mucho más limitada en su contenido, en específico a la información de los abonados como se ha explicado previamente. Así, la orden de presentación no alcanza el contenido de las

[80] "*Art. 218 bis: El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquiera de las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia*"

comunicaciones mientras que el proyecto establece que se debe entregar "*datos o informaciones acerca de las comunicaciones transmitidas o recibidas por ellas*". En virtud de lo dispuesto y dado que tiene menores exigencias que las facultades que se incorporan en el propio proyecto, su alcance no debería extenderse a la totalidad de la información, es decir al contenido de la misma y a la individualización de los participantes, sino a informaciones generales de las comunicaciones que no impliquen un acceso total. Cómo se aterriza esta distinción; sin embargo, es difícil de limitar y tal como está actualmente conceptualizada podría utilizarse para acceder indiscriminadamente a la información virtual de cualquier imputado.

Esto es especialmente preocupante ante la falta de adaptación de los distintos niveles de solicitud de información que ya hace el Convenio ratificado y que no se mencionan en el proyecto. El Comité de Ministros de Europa se preocupó en el instrumento de plasmar varias formas de acercamiento al problema según el nivel de afectación del delito y la proporcionalidad del caso, que parte desde la conservación y exhibición parcial rápida hasta el registro en tiempo real; pasando por la orden de presentación; el registro e información de datos almacenados; la interceptación de datos relativos al contenido e incluso la obtención en tiempo real de datos relativos al tráfico, que presentan sus propios requisitos.

Al contrario, la figura genérica del artículo 16 letra b) del proyecto es la única norma de solicitud de información y no cuenta con parámetro alguno para su determinación. No se señala ninguna exigencia respecto de la gravedad o naturaleza del ilícito ni de mayores límites en las "copias de comunicaciones o transmisiones". Esto es especialmente grave considerando que ni siquiera se contempla la notificación del imputado y que no se extiende lo dispuesto por el artículo 222, que para todos los efectos tiene mayor regulación en atención a la gravedad de la intrusión en el derecho a la vida privada y la inviolabilidad de las comunicaciones establecidas en la propia Constitución Política.

Es por esto por lo que; a nuestro parecer, la figura comentada es profundamente deficiente y peligrosa, siendo un mejor camino el de adoptar las medidas establecidas en el mismo Convenio de Budapest.

c) Modificaciones al artículo 222 del Código Procesal Penal: Se incorpora la conservación de los datos relativos al tráfico, debiendo las empresas concesionarias de servicio público de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también estos últimos mantener con carácter de reservado los metadatos de todos sus usuarios en un plazo no menor a 2 años. Esta disposición ha sido la que ha producido mayor discusión en su tramitación a la fecha y que recuerda lo propuesto por el llamado decreto espía, invalidado por Contraloría.

Primero que todo es fundamental entender el concepto de metadatos y toda la información que comprende. En concreto, y lo señala el propio artículo en análisis, estamos hablando de la información del origen, la localización del punto de acceso a la red, destino, ruta, hora, fecha, tamaño y la duración de la comunicación o el tipo de servicio subyacente de toda comunicación que la comunidad realiza mediante servicios de internet. La relevancia de este tipo de información es clara y permite configurar perfectamente un perfil personal completo de cada individuo y de sus esferas más íntimas de privacidad. Así, el hecho de que instituciones privadas controlen esta información por un plazo indeterminado (mínimo 2 años) es grave.

Actualmente nuestra legislación establece el deber de conservar la información por el plazo de 2 años, pero solo respecto a los datos de IP, no a la extensión aquí contemplada. La determinación del contenido específico y del tiempo que debe estar la información en poder de estas empresas es clave para garantizar la privacidad de todos los ciudadanos y la forma en que se establece por el proyecto no garantiza en lo más mínimo el respeto a estos derechos.

Otra razón para modificar lo propuesto es la notable falta de control respecto a la custodia de los metadatos. Esto porque si bien la Superintendencia de Telecomunicaciones ejerce la supervigilancia de este tipo de instituciones, no se establece ninguna responsabilidad en caso

de filtración, modificación o pérdida de la información. Tampoco se establecen mecanismos de control al efecto, lo que hace aún más peligrosa la conservación de este tipo de información.

4- Modificación a la ley 20.393 *que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica*. Se incluye el listado de delitos aquí establecidos en la responsabilidad penal de las personas jurídicas.

Esta innovación es un elemento interesante y valioso para responder al avance de la utilización de medios digitales con intención fraudulenta y alcances delictivos no solo respecto de particulares sino también de agrupaciones jurídicamente reconocidas e incluso empresas que pueden verse involucradas en este tipo de conductas en lo que correspondería claramente a comportamientos no solo de competencia desleal, sino derechamente delictivos que cumpliendo con las hipótesis dispuestas por la ley 20.393 deberían conllevar la responsabilidad cierta de la personalidad jurídica más allá del perpetrador que individualmente haya concretado el delito.

5- Disposiciones transitorias: La ley comenzará a regir transcurridos 90 días de su publicación y se aplicará solo respecto de delitos cometidos con posterioridad a su entrada en vigencia.

5.- Modificaciones realizadas al texto original

Finalmente, el proyecto de ley aquí presentado fue aprobado por el Senado con fecha 3 de marzo de 2020, pero con una serie de indicaciones levantadas durante su primer trámite constitucional y procesadas por la Comisión de Seguridad Pública. Gran parte de estas indicaciones se hacen cargo de las críticas presentadas en relación al desajuste de sus disposiciones con lo contemplado por el Convenio, además de la mantención del elemento subjetivo de la ley 19.223.

Dentro de las modificaciones más importantes podemos señalar las siguientes:

- En el artículo 5° de falsificación informática se agrega una figura agravada al ser cometida por funcionario público.

- Se crea un nuevo artículo 6°, pasando el original a 7° y así sucesivamente. En este artículo se establece una nueva figura penal: La receptación de datos como "*El que conociendo su origen o no pudiendo menos que conocerlo, almacene, a cualquier título, datos informáticos provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5° sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.*"

- En el artículo 6 original de fraude informático se agrega: "*Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.*"

- Se amplía la atenuante especial de cooperación eficaz.

- El artículo 11 original se amplía considerablemente ya que se suprime la exigencia de participación de una agrupación para solicitar las medidas del artículo 222 al 226 del Código Procesal Penal al Juez de Garantía. Además, **se incorpora la figura del agente encubierto en línea**.

- Se agrega "proveedores de servicios" a las definiciones.

- Se incorpora como eximente penal la figura del *hackeo* autorizado que se realiza para comprobar vulnerabilidades del sistema.

- Sobre las modificaciones al Código Procesal Penal, se cambia el texto original del literal b) para incorporar expresamente la solicitud de datos del suscriptor además de datos relativos al tráfico y al contenido; debiendo contar con autorización judicial respecto de las últimas. Se establece un plazo de 1 año para la conservación de datos

relacionados a los abonados y al tráfico por parte de los proveedores, debiendo proceder a su destrucción luego de tal periodo.

- Se incorporan sanciones para quienes infrinjan el deber de reserva o secreto sobre los datos almacenados por los proveedores.

- Se incluye en su numeral primero, la circunstancia de "*actuar abusando de una posición de confianza en la administración del sistema informático o de ser custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función".*

  Además, en el inciso final se incorpora el aumento de un grado en la pena en los casos que se "*afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley N.º 18.700, orgánica constitucional sobre votaciones populares y escrutinios*".

CAPÍTULO III: MEDIDAS INTRUSIVAS EN LA LEGISLACIÓN NACIONAL.

Como ya revisamos anteriormente, a propósito de los proyectos de adecuación de la legislación nacional al Convenio de Budapest, nuestro ordenamiento jurídico se encuentra muy desactualizado en materia de obtención de evidencia digital, y en general en todo lo que respecta a la utilización de datos digitales en las investigaciones que se llevan a cabo por el Ministerio Público.

Los artículos 180 y 181 del Código Procesal Penal, se refieren a las actuaciones que puede solicitar el Ministerio Público en el marco de la etapa de investigación para el esclarecimiento de los hechos; el inciso segundo del artículo 181 dispone: *"Para el cumplimiento de los fines de la investigación se podrá disponer la práctica de operaciones científicas, la toma de fotografías, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que resultaren más adecuados, requiriendo la intervención de los organismos especializados. En estos casos, una vez verificada la operación se certificará el día, hora y lugar en que ella se hubiere realizado, el nombre, la dirección y la profesión u oficio de quienes hubieren intervenido en ella, así como la individualización de la persona sometida a examen y la descripción de la cosa, suceso o fenómeno que se reprodujere o explicare. En todo caso se adoptarán las medidas necesarias para evitar la alteración de los originales objeto de la operación."*

Las diligencias ya sean de iniciativa fiscal, o bien de parte de alguno de los intervinientes[81] en el proceso, tienen distintas clasificaciones según la doctrina, siendo la más relevante para el efecto de nuestro estudio, la que distingue entre actos intrusivos y no intrusivos[82], según si afectan o no el respeto y protección a la vida privada y pública, a la honra de la persona y de su familia, la inviolabilidad del hogar y de toda forma de comunicación privada, protegidos constitucionalmente; la importancia de esto, tiene relación con el artículo 9 del mismo cuerpo

[81] El artículo 183 de Código Procesal Penal, permite la proposición de diligencias al Ministerio Púbico por parte del imputado u otro de los intervinientes en el proceso, propuesta sobre la que el fiscal deberá pronunciarse en un plazo de 10 días.
[82] CHAHUÁN Sarrás, Sabas. 2012. Manual del Nuevo Procedimiento Penal. Séptima edición. Santiago, Chile. Thomson Reuters. ISBN 978-956-346-103-9.

normativo, el cual señala que en caso de perturbación o privación de alguno de los derechos protegidos por la Constitución se requerirá autorización previa por parte del Juez de Garantía[83]; asimismo, dentro de las diligencias que requieren autorización judicial previa, es posible distinguir aquellas que pueden solicitarse con conocimiento del afectado versus aquellas que pueden solicitarse sin ese conocimiento. La regla general es que las diligencias que requieren de autorización judicial sean comunicadas al imputado, antes de llevarse a cabo. Excepcionalmente se puede disponer **i. Antes de formalizarse la investigación:** cuando la gravedad de los hechos o la naturaleza de la diligencia hagan presumir que el desconocimiento por parte del afectado es indispensable para el éxito de la actuación; **ii**. **Después de formalizada la investigación**: cuando la reserva resulte estrictamente indispensable para la eficacia de la diligencia.

A continuación, revisaremos en específico dos instituciones jurídicas existentes en nuestra legislación, cuya inclusión a nuestro ordenamiento se sitúa a principios del siglo XXI, cuando nuestro país aún no ratificaba el Convenio de Budapest. Estas instituciones, **el agente encubierto y la conservación de datos** no cuentan con un desarrollo acabado de cómo deben operar en el marco de las investigaciones, sino que tienen normas dispersas en distintas leyes, de distintas materias. La primera de ellas implica una evidente perturbación a los derechos a la privacidad de las comunicaciones del afectado por la medida, por lo cual es imprescindible que previo a su ejecución sea visada por el Juez de Garantía de la causa; en el caso del agente encubierto online, España ha determinado que se debe distinguir si el canal en que se empleará será abierto o cerrado, así, en los primeros se puede utilizar una identidad distinta a la real, ya que en estos canales no existe una expectativa legitima de confianza de las identidades, por lo tanto no se requiere una autorización judicial para que fiscales y policías puedan falsear su identidad; en cambio, para las redes de comunicación cerradas, la autorización judicial es imprescindible[84].

[83] De acuerdo con lo dispuesto en la letra a) del artículo 14 del Código Orgánico de Tribunales.
[84] BOSCH, Camila. Op. Cit., 139p.

1.- Conservación de datos e interceptación de comunicaciones.

Cuando nos referimos a la conservación de datos, debemos entender estos últimos de acuerdo con lo establecido en el artículo 1[85] del Convenio de Budapest, donde se definen los conceptos de datos informáticos y de datos relativos al tráfico, de esta manera se podrá obtener la información de conexión, frecuencia, identificar cuentas vinculadas y a través de éstas acceder a comunicaciones, archivos y documentos.

La conservación de datos supone dos elementos importantes, en primer término, que los proveedores de servicios preserven los datos solicitados impidiendo su alteración; y, en segundo término, exige una aplicación restrictiva, solo respecto de aquellos datos debidamente especificados en la solicitud de conservación, evitándose de esta manera que se vulneren garantías fundamentales más allá de lo estrictamente necesario, conforme al principio de proporcionalidad, para el fin de la investigación.

La inclusión de la conservación de datos no está contemplada como tal en nuestra legislación, sino que nos podemos encontrar con lo dispuesto originalmente en la dictación del Código Procesal Penal, específicamente en el artículo 222, la "interceptación de comunicaciones", disposición que otorga la posibilidad de que el Juez de Garantía autorice la interceptación de llamadas telefónicas, y otros medios de telecomunicación. Ya en el año 2004, mediante la Ley 19.927 que "*Modifica el código penal, el código de procedimiento penal y el código procesal penal en materia de delitos de pornografía infantil*" se incorporó, el artículo 113 ter, al Código de Procedimiento Penal, que estableció la posibilidad de que en casos "*que la investigación (por determinados delitos) lo hiciere imprescindible, el juez podrá ordenar la interceptación o grabación de las telecomunicaciones de esa persona o de quienes integraren dicha*

[85] b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función; d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

organización y la grabación de comunicaciones"; el contenido normativo del artículo 113 ter del "antiguo" Código de Procedimiento Penal, coincide con el contenido del artículo 222 del Código Procesal Penal, al cual mediante la mencionada ley incorpora un nuevo inciso 5° que obliga a los proveedores de servicios de internet y de telefonía a mantener bases de datos que permitan a solicitud del Ministerio Público identificar datos de conexión de un determinado usuario *"(…) en el menor plazo posible. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a seis meses*[86]*, de los números IP de las conexiones que realicen sus abonados.".*

En este contexto, es importante revisar La Ley General de Telecomunicaciones (18.168), dictada en el año 1982, la cual se dicta con el fin de separar la regulación de los servicios de telecomunicaciones, de la Ley general de servicios eléctricos, haciéndose cargo del alto desarrollo que ya en los años 80 alcanzaban las telecomunicaciones en el mundo, y nuestro país; así, la Ley comienza entregando el concepto de lo que se entenderá por Telecomunicación como: *"toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos."* Bajo este concepto podemos circunscribir todo tipo de señales de comunicación, ya sea por vía internet, por televisión o telefonía.

El contenido de la Ley es amplio y regula las concesiones de instalación, operación y explotación de servicios de telecomunicaciones (Título II), su explotación y obligaciones de los concesionarios (Título III), los derechos de utilización del espectro eléctrico (Título VI), y las infracciones y sanciones (Título VII), entre otras. En lo que nos convoca, la regulación del Título VII correspondiente a "infracciones y sanciones", en el artículo 36 establece distintas sanciones que van desde la multa hasta la caducidad de la concesión o permiso para aquellos

[86] Hoy, no inferior a 1 año, por Ley 20.526

concesionarios que incumplan sus obligaciones y entreguen un servicio de telecomunicación deficiente.

Por otra parte, el artículo 36 B establece distintos tipos penales, con carácter de acción penal pública, que van desde la operación y explotación, sin autorización, de los servicios e instalaciones de telecomunicación, hasta la interceptación y difusión de comunicaciones obtenidas maliciosamente. Así, el artículo 36 B[87], señala:

"comete delito de acción pública:

b) El que maliciosamente interfiera, intercepte o interrumpa un servicio de telecomunicaciones, sufrirá la pena de presidio menor en cualquiera de sus grados y el comiso de los equipos e instalaciones.

c) El que intercepte o capte maliciosamente o grave ***sin la debida autorización****, cualquier tipo de señal que se emita a través de un servicio público de telecomunicaciones, será sancionado con la pena de presidio menor en su grado medio y multa de 50 a 5.000 UTM.*

*d) La difusión pública o privada de cualquier comunicación obtenida con infracción a lo establecido en la letra precedente, será sancionada con la pena de presidio menor en su grado máximo y multa de 100 a 5.000 UTM[88]."*De esta forma podemos evidenciar la gravedad que implica la interceptación de comunicaciones y la difusión de las mismas, estando establecidas expresamente como delitos en esta ley, y que, como medida de investigación, debe cumplir estrictamente con los requisitos establecidos por la Ley, que a hacen procedente solo en casos restringidos.

La interceptación de comunicaciones y la conservación de datos son medidas polémicas que implican una vulneración al derecho de privacidad de comunicaciones, resguardado

[87] Solo se hará referencia a aquellas infracciones que sean materia de nuestro estudio
[88] Tanto las letras c y d de este artículo fueron incorporadas por la Ley 19.277 del año 1994, que "Introduce modificaciones que indica a la Ley 18.168, General de Telecomunicaciones".

constitucionalmente, en el artículo 19 N°5, el cual señala *"La constitución asegura a todas las personas: 5° La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los* ***casos y formas determinados por la ley".***

Para asegurar esta norma constitucional, se consagró el principio de neutralidad en la red para los consumidores y usuarios de internet en la Ley 20.453, que incorporó el artículo 24 H[89] a La Ley General de Telecomunicaciones (18.168) del año 1982, señalando:

"*Artículo 24 H.- Los proveedores de acceso a Internet serán aquellas personas jurídicas que presten servicios comerciales de conectividad entre usuarios finales o redes de terceros e Internet y estarán sujetos a las siguientes disposiciones:*

a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer tanto a sus usuarios, en el caso del servicio de acceso a Internet, como a los otros proveedores que les contraten servicios de conectividad para sus usuarios propios, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios.

Con todo, los proveedores de acceso a Internet podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red, en el exclusivo ámbito de la actividad que les ha sido autorizada, siempre que ello no tenga por objeto realizar acciones que afecten o puedan afectar la libre competencia. ***Los proveedores de acceso a Internet procurarán preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red****. Asimismo, podrán bloquear el acceso a determinados contenidos, aplicaciones o servicios, sólo a pedido*

[89] También incorporó los artículos 24 I y 24 J a la misma.

expreso del usuario, y a sus expensas. En ningún caso, este bloqueo podrá afectar de manera arbitraria a los proveedores de servicios y aplicaciones que se prestan en Internet.[90]

De esta manera, se establece una obligación para los proveedores de servicio, de entregar un libre acceso a la red y de procurar la privacidad de sus interacciones en la web, entregando protección y seguridad en las mismas. Así, las medidas intrusivas que contempla la legislación chilena operan como una excepción a esta norma, estableciendo el deber de los proveedores de servicios web de entregar datos de los usuarios según el inciso quinto del artículo 222[91] del Código Procesal Penal, así como el contenido de sus comunicaciones y acciones en la web. Aquí se establece que las empresas deberán mantener un registro reservado de los números de IP de las conexiones que realicen sus abonados, por un plazo "no inferior a un año".

Esta normativa se intentó modificar el 13 de junio de 2017, cuando el Ministerio del Interior y Seguridad Pública dictó el polémico Decreto N°866 que "*establece reglamento sobre interceptación de comunicaciones telefónicas y otras formas de telecomunicación, y de conservación de datos comunicacionales*", llamado por algunos "el decreto espía", el cual señalando la necesidad de mejorar el procedimiento de interceptación y conservación de datos, buscaba establecer medidas de alcance general para los distintos proveedores de servicio en esta materia. El reglamento contaba de 16 artículos que establecía el funcionamiento de la interceptación de comunicaciones, el papel que los proveedores jugaban, sus deberes, y formas de proceder en las solicitudes; sin embargo, la redacción del decreto y al hecho de que buscaba regular materias relativas a la privacidad de las comunicaciones mediante un reglamento, cuando tal y como este mismo lo indicaba; en su parte considerativa, son materias de ley. En base a esto, se presentaron una serie de

[90] En el año 2017, la Ley 21.046 modificó la redacción de la norma, manteniendo lo sustantivo respecto la obligación de los proveedores.

[91] Las empresas telefónicas y de comunicaciones deberán dar cumplimiento a esta medida, proporcionando a los funcionarios encargados de la diligencia las facilidades necesarias para que se lleve a cabo con la oportunidad con que se requiera. Con este objetivo los proveedores de tales servicios deberán mantener, en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación será constitutiva del delito de desacato. Asimismo, los encargados de realizar la diligencia y los empleados de las empresas mencionadas en este inciso deberán guardar secreto acerca de la misma, salvo que se les citare como testigos al procedimiento.

requerimientos ante la Contraloría General de la República (Contraloría), de distintas organizaciones que buscaban presentar observaciones sobre la legalidad del reglamento Este organismo finalmente no tomó razón de esta norma, por lo que no entró en vigencia.

A vía ejemplar, el 28 de agosto del 2017 la ONG Derechos Digitales[92], ingresó su petición a la Contraloría en la que se solicitaba que la Contraloría no tomara razón del decreto, declarándolo ilegal. De la misma forma, el 30 de agosto, el Instituto Chileno de Derecho y Tecnología (ICDT), presentó su propio requerimiento ante la Contraloría, en el cual señaló, entre otras cosas que: "*el nuevo Reglamento vulnera los límites formales y materiales de la potestad reglamentaria al transgredir abiertamente la garantía fundamental de la inviolabilidad del hogar y de toda forma de comunicación privada del Art. 19 Nº 5 de la Constitución Política de la República, no solo al entregar competencias para la obtención de datos de comunicaciones a entidades distintas del Ministerio Público, sino también al establecer un sistema de conservación de datos que se aparta del texto de las normas procesales penales en la materia, entrando derechamente a regular materia propias de la competencia del Congreso Nacional, como son las restricciones a los derechos fundamentales."*[93]

Entre las normas más cuestionables de reglamento se encontraba lo referente a:

a) **Ampliación de datos a recolectar**: El artículo 8 del decreto señala que las empresas de telecomunicaciones deberán almacenar "*todos los datos comunicacionales*", los que se detallan en el artículo 10, haciendo una lista que incluye información sobre los participantes de la comunicación, datos de geolocalización y antecedentes que permitan conocer los datos administrativos y financieros. Todo esto es mucho más

[92] DERECHOS DIGITALES. ¿Qué dice el llamado "Decreto espía"? agosto, 2017. [En línea] <https://www.derechosdigitales.org/11400/que-dice-el-llamado-decreto-espia/> [Consulta: 01 de junio de 2020]

[93] INSTITUTO CHILENO DERECHO Y TECNOLOGÍA. Petición a Contraloría General de la República. Agosto, 2017. [En línea] <http://www.icdt.cl/wp-content/uploads/2017/08/peticion-CGR-30agosto.pdf> [Consulta: 01 de junio de 2020]

amplio que lo existente en la norma actual del artículo 222, que se limita a los datos y conexiones de la dirección IP del dispositivo.

b) **Sobre el plazo del almacenamiento:** El artículo 8 del decreto establecía una ampliación del plazo en que los datos comunicacionales deben ser almacenados por el proveedor de servicio, de un año que establece el Código Procesal Penal, a dos años.

Quizás la parte más polémica está en la redacción del artículo 8, el cual señalaba "*Los prestadores de servicios de telecomunicaciones mantendrán y almacenarán por un período no inferior a 2 años, en carácter de reservado y a* ***disposición de la autoridad****, todos los datos comunicacionales a que se alude en este título."* En esta norma como se logra apreciar no se exige la existencia de una orden judicial, y que al hablar de que deben estar a disposición de la autoridad no se hacen especificaciones, lo que podría dar pie a que sea la policía quien solicite estos datos de manera libre. En este mismo sentido, el artículo 1 del decreto establece que la información debe estar a disposición del Ministerio Público y de *"toda otra institución que se encuentre facultada por ley para requerirlo*".

Finalmente, el 24 de noviembre de 2017, la Contraloría General de la República, emite el dictamen N°41.188, que dispone: "*Esta Entidad de Control ha debido abstenerse de dar curso al documento individualizado en el rubro, que "Establece Reglamento Sobre Interceptación de Comunicaciones Telefónicas y de Otras Formas de Telecomunicación, y de Conservación de Datos Comunicacionales", por no ajustarse a derecho*.

En efecto, debe objetarse que diversas disposiciones del señalado reglamento regulan materias propias de ley, como lo son las relativas a la conservación de datos comunicacionales por parte de los prestadores de servicios de telecomunicaciones, y a las atribuciones de los jueces de garantía y del Ministerio Público, excediendo las normas del Código Procesal Penal que se

invocan como fundamento o resultan aplicables"[94]. Cerrando definitivamente la puerta a la regulación por vía de este decreto.

Es necesario hacer presente la importancia de este caso, y la vulnerabilidad a que está expuesta la población respecto el control de datos e información personal por parte de agentes del Estado.

A continuación, analizaremos las leyes en que se encuentra regulada esta herramienta en nuestro país y como se aplica de manera practica en las investigaciones.

a.- Ley 20.000 que sanciona el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas.

En el año 2005 entra en vigencia la Ley 20.000, que reemplaza la antigua ley 19.366 que sanciona el tráfico ilícito de estupefacientes y sustancias sicotrópicas; contempla los delitos y circunstancias agravantes relacionados con el tráfico de drogas; y en su Título II, establece "*Técnicas de Investigación*", contempladas especialmente para la persecución de este tipo de delitos, en específico en la materia que nos convoca, el párrafo 2º titulado *"De la restricción de las comunicaciones y otros medios técnicos de investigación",* dispone:

Artículo 24.- Las medidas de retención e incautación de correspondencia, obtención de copias de comunicaciones o transmisiones, interceptación de comunicaciones telefónicas y uso de otros medios técnicos de investigación, se podrán aplicar respecto de todos los delitos previstos en esta ley y cualquiera sea la pena que merecieren, de conformidad a las disposiciones pertinentes del Código Procesal Penal.

[94]CONTRALORÍA GENERAL DE LA REPÚBLICA. Dictamen N°41.188-17. Noviembre, 2017 [En línea] <https://www.contraloria.cl/pdfbuscador/dictamenes/041188N17/html> [Consulta: 01 de junio de 2020]

Sin perjuicio de lo anterior, no regirá lo dispuesto en el inciso cuarto del artículo 222[95] *de ese Código, en cuanto a indicar circunstanciadamente el nombre y dirección del afectado por la medida, siendo suficiente consignar las circunstancias que lo individualizaren o determinaren.*

Asimismo, no obstante, lo prevenido en el artículo 167 de dicho Código, si las diligencias ordenadas no dieren resultado, el fiscal podrá archivar provisionalmente la investigación hasta que aparezcan mejores y nuevos antecedentes.

De acuerdo con lo establecido por esta disposición, el Ministerio Público podrá solicitar al Juez de Garantía que se autorice la interceptación y grabaciones de comunicaciones de el o los imputados que estén siendo investigados de acuerdo a lo establecido por dicha Ley. Tal como lo indica el inciso primero del artículo 222 del Código Procesal Penal, el Ministerio Público, deberá presentar antecedentes suficientes que funden la solicitud y que acrediten que existen fundadas sospechas de que participó o podría participar en un hecho delictivo que tenga asignada pena de crimen[96]; sin embargo, como indica el citado artículo 24 de la ley 20.000 no será necesario individualizar a los afectados por la medida con el fin de mantener el secreto de la investigación.

Como ya mencionamos, la legislación chilena contemplaba desde 2004 aproximadamente la posibilidad de interceptar y conservar comunicaciones, más de una década antes de adoptar el Convenio de Ciberdelincuencia, de manera que, lo que viene a aportar dicho Convenio en materia de la ley 20.000, es que incorporando su regulación referida a la cooperación internacional en materia de conservación de datos, facilita la obtención de éstos, cuando se encuentren en proveedores o servidores extranjeros, agilizando las actuaciones en materia de investigación, las que con anterioridad a la entrada en vigencia del Convenio, debían hacerse por medio de la Cancillería, haciendo poco efectiva la conservación y obtención de los datos

[95] La orden que dispusiere la interceptación y grabación deberá indicar circunstanciadamente el nombre y dirección del afectado por la medida y señalar la forma de la interceptación y la duración de la misma, que no podrá exceder de sesenta días. El juez podrá prorrogar este plazo por períodos de hasta igual duración, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en los incisos precedentes.

[96] Artículo 21 Código Penal.

para ser utilizados en un procedimiento; mientras que en materia procesal propiamente, incluye una serie de nuevas herramientas y disposiciones para las investigaciones en esta materia.

La utilidad de la norma y los aportes del Convenio son evidentes, dado que el tráfico de drogas suele tener alcances transnacionales, mediante redes dedicadas a la producción y distribución de sustancias ilícitas a nivel internacional. Así, en materia de investigación, por parte del Ministerio Público, es muy típico el contacto con policías y fiscalías extranjeras para la identificación de estas redes, siendo muy común y efectivo contar con la posibilidad de interceptar comunicaciones que sirvan de antecedente ya sea para la captura *in fraganti* de una entrega de drogas, para la facilitación de la implementación de un agente encubierto, o como evidencia dentro de un juicio oral.

b.- Ley 19.974 Sobre el Sistema de Inteligencia del Estado y que crea la Agencia Nacional De Inteligencia.

La ley 19.974 fue promulgada en el año 2001, y tuvo por objetivo regular los sistemas de inteligencia[97] y contrainteligencia[98] del Estado, que tengan por objetivo resguardar en especial la seguridad nacional de las amenazas del terrorismo, crimen organizado y narcotráfico.

El título V de la Ley, titulado "*De los procedimientos especiales de obtención de información*." Contempla en el artículo 24 "a*) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; b) La intervención de sistemas y redes informáticos; c) La escucha y grabación electrónica incluyendo la audiovisual, y d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información*." Lo

[97] El proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones. (artículo 2, letra a)

[98] Aquella parte de la actividad de inteligencia cuya finalidad es detectar, localizar y neutralizar las acciones de inteligencia desarrolladas por otros Estados o por personas, organizaciones o grupos extranjeros, o por sus agentes locales, dirigidas contra la seguridad del Estado y la defensa nacional. (artículo 2, letra b)

anteriormente señalado será procedente sólo cuando los antecedentes que se pretenden obtener aporten al objetivo de proteger y resguardar la seguridad nacional de las amenazas del terrorismo, narcotráfico y crimen organizado; y que provengan de una fuente cerrada, es decir, que no se pueda obtener de fuentes de información abierta al público.

El artículo 24 forma parte del texto original de la ley, y permite que los organismos encargados de inteligencia (policías) intervengan dispositivos electrónicos de uso personal, siempre y cuando se cumpla con los requisitos que exige el artículo 23, y que su intervención sea necesaria para la seguridad nacional; a continuación el artículo 25 exige que los directores o jefes de la secciones de inteligencia soliciten autorización a un Ministro de la Corte de Apelaciones correspondiente al territorio donde se llevara a cabo el procedimiento.

La interceptación de comunicaciones en este caso opera de una manera distinta, ya que los funcionarios de inteligencia no operan por intermedio u órdenes del Ministerio Público, dado que la finalidad única de estas intervenciones debe ser obtener información para mantener la seguridad del país. Esto último ha sido cuestionado a propósito del llamado "Caso Huracán", caso que salió a la luz el año 2018, en el cual funcionarios de la Unidad de Inteligencia de Carabineros de Chile, infiltraron mensajería en los dispositivos móviles de distintos comuneros mapuches, mensajes que fueron posteriormente entregados a la fiscalía para que se iniciara una investigación en su contra y se solicitara su orden de detención; cuando se hizo un control sobre las diligencias se pudo detectar la manipulación de los mensajes y los dispositivos, así como que se habían efectuado numerosas intervenciones en teléfonos móviles de periodistas, actores y políticos[99], sin mediar motivos plausibles para sospechar que pusieran en riesgo la seguridad del Estado, y sin contar desde luego, con autorización correspondiente de un Ministro de Corte. Este caso demostró la falta de regulación con que cuenta la Ley, y la libertad con que funcionan las unidades de inteligencia respecto la privacidad de los ciudadanos.

[99] BIBLIOTECA DE CONGRESO NACIONAL DE CHILE. Asesoría técnica parlamentaria "Caso Huracán". Mayo, 2018. [En línea] <https://www.camara.cl/pdf.aspx?prmTIPO=DOCUMENTOCOMUNICACIONCUENTA&prmID=70045> [Consultado: 01 de junio de 2020]

c.- 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.

Promulgada el 5 de enero de 2004, esta Ley vino a modificar distintos cuerpos normativos, con el fin de facilitar las investigaciones y aumentar las penas relacionadas a los delitos de producción de material pornográfico infantil, y otros delitos relacionados con menores.

En el Código Penal, se introdujo el artículo 369 ter[100]. El cual contempla la posibilidad de que el Ministerio Público solicite la interceptación de todas las telecomunicaciones respecto una persona o una organización, cuando existan sospechas fundadas de que esta medida resulte **imprescindible** para los resultados de la investigación, en delitos de producción de material pornográfico infantil, y facilitación de prostitución de menores[101], la autorización por el Juez de Garantía, y la práctica de la diligencia misma se llevará a cabo conforme a lo establecido por las normas de los artículos 222 y 225 del Código Procesal Penal, normas que también fueron modificadas por esta Ley.

Respecto el artículo 222 del Código Procesal Penal, se incorporó la exigencia a los proveedores de servicios de mantener un listado de los rangos autorizados de direcciones IP, además de un

[100]Art. 369 ter. "Cuando existieren sospechas fundadas de que una persona o una organización delictiva hubiere cometido o preparado la comisión de alguno de los delitos previstos en los artículos 366 quinquies, 367, 367 ter, 374 bis, inciso primero, y 374 ter, y la investigación lo hiciere imprescindible, el tribunal, a petición del Ministerio Público, podrá autorizar la interceptación o grabación de las telecomunicaciones de esa persona o de quienes integraren dicha organización, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos y la grabación de comunicaciones. En lo demás, se estará íntegramente a lo dispuesto en los artículos 222 a 225 del Código Procesal Penal. Igualmente, bajo los mismos supuestos previstos en el inciso precedente, podrá el tribunal, a petición del Ministerio Público, autorizar la intervención de agentes encubiertos. Mediando igual autorización y con el objeto exclusivo de facilitar la labor de estos agentes, los organismos policiales pertinentes podrán mantener un registro reservado de producciones del carácter investigado. Asimismo, podrán tener lugar entregas vigiladas de material respecto de la investigación de hechos que se instigaren o materializaren a través del intercambio de dichos elementos, en cualquier soporte.
La actuación de los agentes encubiertos y las entregas vigiladas serán plenamente aplicables al caso en que la actuación de los agentes o el traslado o circulación de producciones se desarrolle a través de un sistema de telecomunicaciones.
Los agentes encubiertos, el secreto de sus actuaciones, registros o documentos y las entregas vigiladas se regirán por las disposiciones de la ley Nº20.000."

[101] artículos 366 quinquies, 367, 367 bis, 367 ter, 374 bis, inciso primero, y 374 ter. Del Código Penal.

registro de las conexiones que realicen sus abonados, de manera de tener disponible la información para investigaciones pertinentes.

Originalmente, la norma contemplaba que el registro mantuviera la información de conexión por un plazo mínimo de 6 meses, sin embargo, en el año 2011 esto se modificó ampliando el rango de duración de los registros a mínimo 1 año[102].

Además, como norma de protección a los menores, se estableció que los dispositivos incautados durante las investigaciones quedaran en manos del Servicio Nacional de Menores, o de organismos policiales especializados.

La incorporación de estas normas; junto con las demás disposiciones, están dispuestas para facilitar la obtención de archivos y conversaciones que puedan servir de base para una acusación por parte de Ministerio Público; su incorporación en el año 2004 tiene que ver con la masificación de este tipo de delitos y las facilidades que brinda internet para su comisión, y la falta de norma expresa que permitiría a los fiscales interceptar dispositivos como computadores y celulares en los que se almacenaba la información y medios de prueba para estos delitos.

d.- Ley 19.913 Crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos.

Publicada el 12 de diciembre de 2003, la Ley 19.913, crea la Unidad de Análisis Financiero (UAF) con el fin de prevenir la utilización del sistema financiero para la comisión de los delitos que contempla la misma[103]; entre sus normas se encuentra, a partir del artículo 31, la forma de proceder en la investigación de estos delitos, e incluye el secreto de la investigación respecto terceros, y respecto el imputado hasta por 6 meses, plazo renovable.

[102] Ley 20.526

[103] Art. 27 letra a y b, correspondiente al lavado y blanqueo de activos. Y art. 28 correspondiente a asociación ilícita con fines de blanqueo y lavado de activos.

Por otra parte, el artículo 33 contempla en su letra a) lo siguiente:

"*a) Investigación: se comprenden, especialmente, la colaboración de organismos del Estado, la facultad del Ministerio Público para efectuar actuaciones fuera del territorio nacional o sin previo conocimiento del afectado y la cooperación internacional en general; levantamiento del secreto bancario; gratuidad de los antecedentes requeridos durante la investigación; técnicas especiales de investigación, como la entrega u operación vigilada, la utilización de agentes encubiertos e informantes, la interceptación de comunicaciones y demás medios técnicos; protección de las personas que hayan colaborado con la investigación, incluyendo el resguardo de su identidad e imagen, cambio de identidad, secreto de determinadas actuaciones, registros o documentos como medida de protección cuando exista riesgo para su seguridad, sanciones en caso de infracción, y posibilidad de prestar testimonio de manera anticipada;*"

Respecto de los delitos contemplados en el artículo 27 y 28, se estableció la posibilidad de utilizar distintas herramientas de cooperación institucional e internacional para el curso de las investigaciones que se den en el marco de esta Ley, permitiendo la asistencia de instituciones públicas y privadas que faciliten los procedimientos, debido a que los delitos contemplados en esta Ley, movilizan grandes sumas de dinero a través de distintos Estados, ya sea en su origen ilícito o bien en su destino, con el fin de evadir impuestos y eludir la acción de la justicia.

2.- Agente Encubierto.

En Chile, la primera inclusión del agente encubierto a la legislación nacional fue en 1995 con la ley N°19.366[104], antigua ley que sancionaba el tráfico ilícito de estupefacientes y sustancias sicotrópicas. Los problemas que tenía el concepto de agente encubierto en dicha ley se referían a que no especificaba el ámbito de actuación de los agentes, y aún más grave, no limitaba en términos de responsabilidad penal las actuaciones de carácter delictivo de los

[104] Artículo 34 inciso 2: *"Se entiende por agente encubierto el funcionario policial que, debidamente autorizado por sus superiores, oculta su identidad oficial y se involucra o introduce en las organizaciones delictivas simulando ser parte de ellas o estar interesado en la comisión del delito que se investiga, con el propósito de identificar a los partícipes o recoger las pruebas que servirán de base al proceso penal."*

agentes, con ocasión de su encomienda. En el año 2005, con la entrada en vigencia de la Ley 20.000, que reemplazó la ley 19.366, la definición de agente encubierto cambió, y se incluyó en el artículo 25 inciso 2º y 3° como *"el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación.*

El agente encubierto podrá tener una historia ficticia. La Dirección Nacional del Servicio de Registro Civil e Identificación deberá otorgar los medios necesarios para la oportuna y debida materialización de ésta."

Esta herramienta no estaba contemplada para otro tipo de investigaciones distintas de las relacionadas con el tráfico de drogas; a diferencia del derecho comparado donde se comenzó a desarrollar investigaciones en el plano informático utilizando la herramienta del agente encubierto online, definido como "*empleado o funcionario público que, voluntariamente, y por decisión de una autoridad judicial, se infiltra en la Red con el fin de obtener información sobre autores de determinadas prácticas ilícitas producidas a través de la red 'mediante' la ocultación de la verdadera identidad policial, con el fin de establecer una relación de confianza que permita al agente integrarse durante un periodo de tiempo prolongado en el mundo en el que los 'ciberdelincuentes' actúan, con la finalidad primordial, igualmente oculta, de obtener la información necesaria para desenmascarar a los supuestos criminales*"[105]. Esto probó ser efectivo mediante; por ejemplo, las operaciones en las que un agente policial se infiltraba en una red de distribución de material pornográfico infantil, con una identidad falsa y de esta manera podía acceder a información de distintos usuarios, lo que permitiría desbaratar bandas organizadas de pederastia on-line[106].

[105] VALDIVIESO Villanueva. Laura. 2016. Las diligencias de investigación tecnológica y su aplicación práctica en el Orden Jurisdiccional Penal. Trabajo de Fin Máster del Título Propio de la USAL "Máster en acceso a la abogacía". Universidad de Salamanca. 13p.

[106] CAROU Gracia, Sara. 2018. El agente encubierto como instrumento de lucha contra la pornografía infantil en internet. Cuadernos de la Guardia Civil N°56. 23p. ISSN: 2341-3263.

A pesar de esto, desde comienzos de los años 2000 en nuestro país se incluyó la posibilidad de utilizar agentes encubiertos en investigaciones distintas a las relacionadas con tráfico de drogas; ampliando paulatinamente su utilización.

A continuación, analizaremos la incorporación del agente encubierto en distintas normativas nacionales, y cómo se verían modificadas por la incorporación de las figuras del Convenio de Budapest:

a.- Ley 20.000 que sanciona el Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas.

Como ya lo señalamos, el artículo 25 de la Ley 20.000 contempla entre otras herramientas, al agente encubierto, la importancia de esta regulación es muy alta, dado que como veremos más adelante corresponde a la norma a que otros cuerpos normativos se remitirán para citar dicha institución. Sin embargo, no contempla al agente encubierto en su modalidad online.

La naturaleza y estructura del delito de tráfico implica que el funcionario policial se infiltra en una organización criminal, previa autorización judicial, con una identidad falsa, con el fin de recabar información y antecedentes suficientes para la investigación que se lleva a cabo. Esta idea de agente encubierto cumple con los presupuestos establecidos en la legislación española y el proyecto de ley argentino. El proyecto chileno, revisado en el capítulo anterior, que ingresó a la cámara de del Senado el 25 de octubre de 2018, contempla en el inciso 2do del artículo 11:

"*De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de* ***agentes encubiertos*** *e informantes, en la forma regulada por los artículos 23 y 25 de la ley N°20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos o comprobarlos."*

Como vemos, nuevamente el proyecto se remite a la regulación establecida por la Ley 20.000, sin establecer mayor diferencia o regulación especial respecto el agente encubierto online.

b.- Ley 19.913 que Crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos.

El título III de la Ley sobre "disposiciones varias", en su artículo 33, letra a) autoriza la utilización de todas las herramientas que contempla la Ley contra el tráfico de drogas a propósito de la investigación de los delitos que establece la Ley 19.913. Como ya señalamos, en lo que a investigación se refiere, la regulación de las herramientas que contempla el artículo 33 letra a) se remite a lo señalado en la Ley 20.000, sin dar mayor desarrollo de las instituciones, y desde luego, sin mencionar la utilización de un agente informático online.

c.- Pornografía Infantil

El Código Penal en su artículo 369 ter inciso segundo señala que el tribunal podrá autorizar, a petición del Ministerio Público, la intervención de agentes encubiertos en la investigación de delitos contemplados en los artículos 366 quinquies, 367, 367 ter, 374 bis, inciso primero, y 374 ter, que contemplan delitos sexuales en donde se vean involucrados menores de edad; esta norma incorporada en por la ley 19.927 del año 2004, ley que incorporó distintos tipos penales referidos al desarrollo de material pornográfico infantil, y con el fin de fortalecer las investigaciones de Ministerio Público, incluye la posibilidad de que con la autorización del Juez de Garantía se autorice la intervención de agentes encubiertos, cuando exista la sospecha de que una persona individual, o bien una organización delictiva hubiera cometido, o bien, preparado la comisión de uno de los delitos ya mencionados. Esto implica que tal como indica el inciso segundo del artículo 369 ter, el agente policial que actúa en el marco de una investigación de este tipo de delitos tendrá a su disposición material con el fin de realizar

entregas vigiladas[107] que permitan identificar a clientes, distribuidores y redes en general, así como su funcionamiento.

"*Igualmente, bajo los mismos supuestos previstos en el inciso precedente, podrá el tribunal, a petición del Ministerio Público, autorizar la intervención de agentes encubiertos. Mediando igual autorización y con el objeto exclusivo de facilitar la labor de estos agentes, los organismos policiales pertinentes podrán mantener un registro reservado de producciones del carácter investigado. Asimismo, podrán tener lugar entregas vigiladas de material respecto de la investigación de hechos que se instigaren o materializaren a través del intercambio de dichos elementos, en cualquier soporte*" (inciso 2do. Artículo 369 ter)

La particularidad de este inciso referido a la intervención de agentes encubiertos es su frase final, donde se incorpora la posibilidad de utilizar cualquier soporte como medio de intercambio, lo cual nos permite hablar de un agente que opera de manera online, dadas las características que tienen los delitos mencionados y su operación principalmente a través de la Red.

[107] *"la circulación autorizada por el Ministerio Público, en el territorio nacional (salgan de él o entren en él), de una remesa de drogas tóxicas, estupefacientes, sustancias psicotrópicas, precursores o sustancias químicas esenciales, o los instrumentos que hubieren servido o pudieren servir para la comisión de alguno de los delitos sancionados en la ley de drogas y sus efectos, sin interferencia de la misma, pero bajo la vigilancia de la autoridad, con el fin de identificar o descubrir a las personas involucradas en la comisión de algún delito relativo a dichas drogas, conocer sus planes, evitar el uso ilícito de las especies referidas o prevenir y comprobar cualquiera de tales delitos".* Definición contenida en el Oficio FN (Fiscal Nacional) N° 65, referido en específico a el tráfico de drogas, sin embargo, nos permite identificar los elementos importantes de este método utilizado por las policías; en primer lugar: la existencia de una autorización previa por parte del Ministerio Público de que circule el objeto de la operación; en segundo lugar: la no interferencia de la autoridad y policía, pero bajo vigilancia, lo que nos permite diferenciarla de la entrega controlada; y en tercer lugar: permite la identificación de personas involucradas, así como conocer sus planes.

CAPÍTULO IV: DERECHO COMPARADO.

Actualmente el Convenio ha sido ratificado por un total de 62 países, 21 de los cuales corresponden a Estados fuera del Consejo de Europa[108]. Procederemos a analizar cómo se encuentra la implementación del Convenio de Budapest en los siguientes sistemas de interés: España, Argentina, Uruguay y Colombia. Esta muestra ha sido seleccionada; tal como se verá, con el fin de contrastar distintas realidades y etapas de legislación en la materia.

Con el objetivo de sistematizar el presente análisis, hemos dividido el estudio en las siguientes categorías ya utilizadas para el estudio nacional:

1. Contexto jurídico de ciberdelincuencia.

2. Etapa de implementación del Convenio de Budapest e hitos de su tramitación nacional.

3. Declaraciones y reservas efectuadas al Convenio.

4. Estado de la normativa interna de adecuación del Convenio.

1.- España.

a.- Contexto jurídico de ciberdelincuencia.

Regulación sustantiva

La regulación interna de los delitos informáticos se encuentra en el Código Penal español, en distintos títulos según el bien jurídico protegido. Para efectos de su categorización y estudio utilizaremos la clasificación de los delitos informáticos empleada por el Observatorio Español

[108] Argentina, Australia, Cabo Verde, Canadá, Chile, Colombia, Costa Rica, República Dominicana, Ghana, Israel, Japón, República de Mauricio, Marruecos, Panamá, Paraguay, Perú, Filipinas, Senegal, Sri Lanka, Tonga y Estados Unidos. Lista completa y actualizada. [En línea] <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ef9Uje9G> [Consulta: 01 de junio de 2020]

de Delitos Informáticos[109], especificando para aquello las disposiciones aplicables y los elementos pertinentes en materia de ciberdelincuencia respecto de cada una de las siguientes categorías:

- Acceso e interceptación ilícita: Art. 197 a 201. Se encuentran figuras como el descubrimiento y revelación de secretos o la comercialización de dispositivos para la comisión de tales delitos; con agravantes para la comisión por funcionarios públicos y tenedores de información de terceros.

Además, en los Art. 278 a 286 se regulan delitos relativos al mercado y los consumidores (espionaje industrial) como la comisión del delito de acceso ilícito para descubrir o revelar "secretos de empresa" o de transmisión de información que atente contra la libre competencia.

- Interferencia en los datos y en el sistema: Arts. 263 a 267 Se regula principalmente el daño grave a datos o programas informáticos; la interrupción grave a un sistema informático y la comercialización de dispositivos electrónicos para aquello, contemplando incluso la responsabilidad de personas jurídicas en la comisión de estos delitos.

- Fraude informático: Arts. 248 a 251. Se enmarca plenamente en la regulación del delito de estafa, donde se pena además la utilización indebida de tarjetas bancarias.

- Falsificación Informática: Arts. 390 a394 que regulan la falsificación documental en general, contemplando la hipótesis de falsificación telegráfica por medio de servicios de telecomunicación. Además; el Art. 399 bis regula la falsificación de tarjetas bancarias y el Art. 400 sanciona la comercialización de programas informáticos para cometer las falsificaciones descritas.

[109] OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS. Ciberdelitos. [En línea] <https://oedi.es/ciberdelitos/> [Consulta: 01 de junio de 2020]

- Delitos sexuales: Arts. 181 a 189. La regulación general de delitos sexuales aplica a la comisión por medios informáticos en figuras como abuso sexual, exhibicionismo y provocación a menores o la venta, difusión o exhibición de material pornográfico de menores de edad o personas con discapacidad. Además, se contempla en el Art. 183 ter la figura de "*grooming*" o engaño pederasta, que consiste en el contacto por medios electrónicos con un menor para concertar un encuentro sexual u obtener material pornográfico.

- Contra la propiedad intelectual e industrial: Arts. 270 a 277. Lo particular de la regulación de estos delitos es la incorporación expresa a quien; con ánimo de obtener un beneficio económico, facilite el acceso a un enlace de internet para acceder a obras objeto de propiedad intelectual, debiendo el juez ordenar la interrupción del sitio de internet. Se sanciona; además, el almacenamiento intencionado de obras de propiedad intelectual.

- Contra la honra: Arts. 205 a 210 que regulan las injurias y calumnias, con una figura agravada por la comisión "con publicidad", donde sería aplicable; bajo ciertas condiciones, su realización mediante redes sociales abiertas.

- Delitos contra la salud pública: Arts. 362 quater y 363 que sancionan a quien ofrezca por medios de gran escala medicamentos, sustancias activas, productos sanitarios u otros productos al margen de la normativa sanitaria.

- Amenazas y coacciones: Arts. 169 a 172 que regulan las figuras generales cuya comisión podría fácilmente realizarse por medios electrónicos y el Art. 172 ter contempla además la figura de acoso por "cualquier medio de comunicación" y la utilización indebida de datos personales.

Regulación procesal

Durante el año 2015 la normativa procesal penal tuvo una reforma importante en España. En particular, en el mes de octubre se dictaron dos leyes relevantes a nuestros efectos; por un lado, la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal "para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". Esta ley tuvo como principal objetivo "el fortalecimiento de los derechos procesales de conformidad con las exigencias del Derecho de la Unión Europea y la regulación de las medidas de investigación tecnológica en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución."[110] Esta ley reguló las siguientes materias: derecho de defensa del investigado (término que sustituye a "imputado" a partir de la nueva Ley de Enjuiciamiento Criminal); el agente encubierto informático[111]; la prisión incomunicada[112]; la detención preventiva y derechos del detenido[113]; medidas de investigación limitativas de los derechos constitucionales mediante autorización judicial tales como la interceptación de las comunicaciones telefónicas y telemáticas; la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos; la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen; el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos.

Además, en octubre de 2015 a su vez se dio lugar a la Ley 41/2015 de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales. Esta ley; complementaria con la anterior, se hace cargo de la reforma de aquellas materias que no requieren ley orgánica "y que son las siguientes: a) la necesidad de establecer disposiciones eficaces de agilización de la justicia penal con el fin de evitar dilaciones indebidas, b) la previsión de un procedimiento de decomiso autónomo, c) la

[110] BOLETÍN oficial del Estado. Núm. 239. Sec. I. 90192p. BOE A-2015-10725. [En línea] <https://www.boe.es/]> [consulta: 01 de julio de 2020]
[111] En apartados 6 y 7 del artículo 282 bis de la Ley de Enjuiciamiento Criminal.
[112] Mediante modificación al artículo 509 de la Ley de Enjuiciamiento Criminal. Además de prohibiciones a derechos mínimos del detenido como el de contactar abogado en el artículo 527.
[113] Mediante modificación al artículo 520 de la Ley de Enjuiciamiento Criminal.

instauración general de la segunda instancia, d) la ampliación del recurso de casación y e) la reforma del recurso extraordinario de revisión"[114]. Dentro de las modificaciones concretas se encuentras aquellas que tienden a evitar lo conocido como macroprocesos mediante la limitación de acumulación por conexión de causas penales[115]; el establecimiento de plazos vinculantes y realistas de instrucción[116]; normas autónomas de decomiso[117]; recurso de apelación para fallos de Audiencias Provinciales o la Sala de lo Penal de la Audiencia Nacional en primera instancia[118]; reforma al recurso de casación[119] y la incorporación de una causal del recurso de revisión por cumplimiento de sentencia del Tribunal Europeo de Derechos Humanos[120].

Estas reformas presentaron una importante resistencia política y social en su tramitación, dado que el proyecto incluso incorporaba la posibilidad de aplicar parte de las medidas procesales señaladas sin autorización judicial, lo que finalmente se revirtió. Aun así, la reforma por ley orgánica contiene normativa que produce preocupación en el campo de los derechos humanos del imputado (investigado). Por ejemplo, se establece la posibilidad de prisión incomunicada hasta 5 días (prorrogables por otros 5 en caso de ciertos delitos) donde la persona privada de libertad no tendría si quiera el derecho a contactar un abogado "si así lo justifican las circunstancias del caso", medida que sería compatible con la prisión preventiva y que de hecho tendría requisitos similares. Además, las medidas procesales señaladas anteriormente tendrían una aplicación muy amplia ya que procederían ante cualquier delito cometido mediante medios informáticos, estableciendo afecciones profundas contra los derechos del investigado tales como la instalación de un virus troyano de seguimiento e incluso control en sus aparatos sin distinción de la gravedad del delito; por lo que incluso podrían proceder ante injurias o calumnias emitidas por redes sociales.

[114]BOLETÍN oficial del Estado. Núm. 239, 6 de octubre de 2015, pp. 90220 a 90239. BOE A-2015-10726. [En línea] <https://www.boe.es/eli/es/l/2015/10/05/41]> [consulta: 01 de julio de 2020]
[115] Mediante modificación del artículo 17 de la Ley de Enjuiciamiento Criminal.
[116] Mediante modificación al artículo 324 de la Ley de Enjuiciamiento Criminal.
[117] Mediante modificación al TÍTULO III ter de la Ley de Enjuiciamiento Criminal.
[118] Nuevo artículo 846 ter de la Ley de Enjuiciamiento Criminal.
[119] Mediante modificación a los artículos 847 y 848 de la Ley de Enjuiciamiento Criminal.
[120] Mediante modificación al artículo 954 de la Ley de Enjuiciamiento Criminal.

De esta forma, la Ley de Enjuiciamiento Criminal regula en su título VIII las medidas de investigación restrictivas. Esta ley ha pasado por diversas modificaciones que le han permitido estar en un nivel de desarrollo avanzado, regulando una diversidad importante de figuras relacionadas a la ciberdelincuencia, varias de las cuales no se encuentran incorporadas en el Convenio de Budapest.

Así, se regula de forma específica en el Capítulo IV (artículos 588 bis a y siguientes) las "*Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de la imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos*".

Se establece que estas medidas requieren autorización judicial en plena sujeción a los principios de especialidad, excepcionalidad, necesidad y proporcionalidad de la medida. Estas medidas se podrán ejecutar en secreto y se llevarán a cabo aunque afecten a terceros, según se determina por cada medida en específico.

Sobre la interceptación de las comunicaciones telefónicas y telemáticas, se limita esta medida a delitos dolosos castigados con penas de hasta al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal; delitos de terrorismo o delitos cometidos a través de instrumentos informáticos.

Luego, el artículo 588 ter d. establece la posibilidad de solicitar judicialmente las siguientes medidas: a) El registro y la grabación del contenido de la comunicación. b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza. c) La localización geográfica del origen o destino de la comunicación. d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación.

Se regula el deber de colaboración de los prestadores de servicios de comunicaciones so pena de incurrir en el delito de desobediencia. El plazo de estas medidas es de hasta 3 meses prorrogables por el mismo tiempo, hasta un máximo de 18 meses.

Terminada la vigencia de la medida y alzado el secreto, se entregará copia de las grabaciones y transcripciones a las partes. En caso de que haya contenido relacionado a la vida íntima de las personas se entregará sin incluir aquello, con expresa constancia de que se excluyó. Luego, cada parte podrá solicitar la inclusión de copias de comunicaciones que estime relevantes y hayan sido excluidas.

En el artículo 588 ter k. se regula la medida de solicitar por la policía los datos del abonado a raíz de una dirección IP detectada en la comisión de un delito, previa autorización judicial. Además, se contempla la captación de códigos de identificación de dispositivos, mediante la utilización de artificios técnicos en aquellos casos en que no se tenga conocimiento del número IP (588 ter I). Una vez obtenidos estos datos se puede solicitar autorización judicial para la realización de otras medidas intrusivas. En caso de necesitar el número de una persona o a la inversa, la fiscalía o policía podrá requerirlo directamente a los prestadores, quienes se encontrarán obligados a entregar tal información.

Se contempla además la posibilidad de solicitar judicialmente la realización de grabaciones a comunicaciones de imputados en lugares abiertos o incluso cerrados, debiendo cumplir con los requisitos de acceso a estos lugares además de los específicos: se exige que esta grabación esté vinculada a un encuentro particular del imputado con otras personas, habiendo indicios de que aportará datos esenciales. Será aplicable solo cuando los hechos constituyan delitos de al menos 3 años de prisión o cometidos por una organización criminal o delitos terroristas. Se podrá complementar con imágenes si así lo autoriza el juez. Se regula aparte la captación de imágenes sin autorización judicial siempre y cuando sea en espacios públicos.

Otra medida contemplada en la ley es la utilización de dispositivos o medios técnicos de seguimiento y localización. Requiere autorización judicial y podrá ser concedida hasta 3 meses, prorrogable por igual tiempo hasta un máximo de 18 meses.

El acceso a dispositivos de almacenamiento masivo de información requisados durante registro domiciliario o en fuera del domicilio del imputado requerirá de autorización judicial expresa.

Se permite el registro remoto sobre equipos informáticos incluso mediante la instalación remota de un software (troyano) sin conocimiento del titular para una amplia categoría de delitos: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. Si los agentes creyeran que los datos buscados se encuentran en otro dispositivo pondrán en conocimiento de esto al juez, quien podrá ampliar la medida. El plazo máximo de la medida es de un mes, prorrogable hasta 2 veces por el mismo plazo.

Finalmente el capítulo X regula las medidas de aseguramiento, incluyendo la conservación de datos mientras se obtiene autorización judicial, por un plazo de 90 días prorrogables una sola vez por el mismo plazo. Esta medida podrá llevarse a cabo sin autorización judicial por la fiscalía o las policías.

Además de estas medidas, debemos mencionar la regulación del agente encubierto informático, contemplado en el artículo 282 bis; quien tiene autorización legal para intercambiar o enviar por sí mismo archivos ilícitos. En general el agente encubierto se permite solo respecto de actividades relacionadas a delincuencia organizada, por un plazo de 6 meses prorrogables según lo determine el juez o el Ministerio Fiscal. Además, durante el curso de la investigación el juez competente podrá autorizar la obtención de imágenes y grabación de reuniones del agente, incluso en lugares cerrados.

b.- Etapa de implementación del Convenio de Budapest e hitos de su tramitación nacional.

España concurrió a la firma del Convenio de Budapest con fecha 23 de noviembre de 2001. Contando con la autorización interna de las Cortes Generales (Congreso) según lo dispuesto por el artículo 94 de la Constitución Española y se procedió a su promulgación en el año 2010, publicado en el Boletín Oficial de Estado (BOE) número 226 de 17 de septiembre de 2010.

c.- Declaraciones y reservas efectuadas al Convenio.

Al ratificar el instrumento internacional; con fecha 3 de junio de 2010, España se limitó a realizar una Declaración consistente en reconocer a Gibraltar como un territorio no autónomo, dependiente del Reino Unido y en proceso de descolonización. Esta declaración fue introducida a su vez en el convenio de adhesión al Marco BEPS de la UCDE y va en la línea de reiterar lo dispuesto por el tratado de Ultrecht de 1713[121] con especial consideración al actual proceso de autonomía en discusión. España no reservó ninguna disposición del Convenio.

d.- Estado de la normativa interna de adecuación del Convenio.

Dado que España promulgó el Convenio ya en el año 2010, las medidas de adecuación adoptadas se encuentran incorporadas plenamente en su legislación, lo que ha sido expuesto en el punto i) del presente acápite. Sin perjuicio de aquello, actualmente se estudia una gran reforma a su sistema procesal penal, la que se encuentra pendiente a partir de un borrador elaborado por el Ministerio de Justicia en 2013 con el objetivo de sustituir la ley de Enjuiciamiento Criminal de 1882.

2.- Argentina.

a.- Contexto jurídico de ciberdelincuencia.

Argentina cuenta con regulación muy desarrollada sobre protección de los datos personales a través la Ley 25.326 del año 2000. Durante el año 2008 se realizó una revisión preliminar del

[121] Tratado firmado por las coronas de España, Gran Bretaña y Países Bajos mediante el cual; luego de 12 años de Guerra de Sucesión Española, se cedió el control de Gibraltar a Gran Bretaña; situación que se ha mantenido con diversas disputas territoriales a través de los años.

Convenio de Budapest y se determinó la necesidad de adecuar la legislación nacional de forma previa[122]. Así, se dio lugar a la Ley 26.388 de 2008 que modifica el Código Penal argentino y moderniza varias disposiciones incorporando un catálogo de delitos informáticos tales como el acceso ilegítimo a bancos de datos personales además de su distribución; la vulneración de datos o sistemas informáticos; la interrupción de comunicaciones; entre otros. Además, amplió la significación de ciertos conceptos empleados en el Código para incorporar de mejor forma elementos digitales[123].

Además, en 2013 se sancionó la Ley de *grooming* 26.904 con penas de cárcel para el que contacte por medio de cualquier tecnología de transmisión de datos a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual.

En materia procesal el análisis es más complejo toda vez que Argentina es un Estado Federal y cada Provincia (23) cuenta con una normativa procesal autónoma. En materia nacional rige lo dispuesto por el Código Procesal Penal de la Nación en su Libro II Título III que fue modificado y actualizado en ciertas materias por la Ley 25.760 de 2003 mediante la cual se amplió la intervención de las comunicaciones no solo a la telefónica y se posibilitó la utilización de medios electrónicos en la comunicación de allanamiento. Si bien se consagra el principio de libertad de prueba en el artículo 206 del Código Procesal Nacional (con excepción del estado civil), no existe mayor regulación general sobre medios informáticos, su obtención conservación y rendición; debiendo acudir a regulación local para encontrar mayor avance al respecto, en efecto:

"*Algunos pocos códigos procesales admiten explícitamente el uso de medios de prueba electrónicos. También, la posibilidad de realizar notificaciones electrónicas, comunicaciones y exhortos.*

[122] Mensaje del Proyecto de Ley enviado por el Ejecutivo para la ratificación del Convenio de Budapest, página 2.
[123] En su artículo primero se amplía el concepto de "documento", "firma" e "instrumento privado".

Solamente la Ciudad de Buenos Aires y la Provincia de Chubut cuentan con ordenamientos jurídicos procesales avanzados que contemplan el uso de medios digitales en la administración de justicia. El recientemente aprobado Código Procesal Penal de la provincia de Entre Ríos, admite para algunas medidas probatorias específicas el uso de medios electrónicos: reconocimiento de voz, reconocimiento por imágenes, testimonial especial filmada, y el principio general establecido en el artículo 300 que admite la filmación de otros actos procesales."[124]

A partir del año 2012 se vio un avance condicionado por los acordados de la Corte Suprema que extendió parte del proceso de la Ciudad Autónoma de Buenos Aires al sistema general de recursos en que interviniera la Corte[125].

b.- Etapa de implementación del Convenio de Budapest e hitos de su tramitación nacional.

Argentina fue invitada a adherirse al Convenio en septiembre de 2010. En marzo de 2017 se ingresa el proyecto de ley para ratificar el Convenio y el poder legislativo de la República Argentina lo aprobó el 22 de noviembre del año 2017, convirtiéndose en la Ley 27.411.

c.- Declaraciones y reservas efectuadas al Convenio.

a) Reserva del artículo 6.1. b[126]: Se fundamenta en que se sanciona la posesión con intención de utilización con fines delictivos según lo descrito por el artículo 6, lo que se estimó una anticipación de la sanción toda vez que no cumple si quiera con los requisitos de la tentativa.

[124] RIVOLTA, Mercedes. 2007. Medios de prueba electrónicos: estado de avance en la legislación argentina. Sistema Argentino de Información Jurídica. Acceso electrónico ID: DACC070049, [En línea] <www.saij.jus.goc.ar> [Consulta: 01 de julio de 2020]
[125] PINNACCHIO, María – CLARA, Ángela. 2017. Los desafíos que las tecnologías plantean incorporarse a los procesos judiciales. ID: DACF170419 [En línea] <www.saij.gob.ar> [Consultado: 01.06.2020]
[126] "La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal"

b) Reserva del artículo 9.1.d, 9.2.b y 9.2.c[127]: La ley 26.388 de delitos informáticos incorporó, modificando el artículo 128 del Código Penal, la sanción contra el financiamiento, ofrecimiento, comercialización, publicación, facilitación, divulgación o distribución de pornografía infantil. La adquisición no está contemplada en el artículo por lo que quedaría fuera de sanción penal. Estaría incorporado lo dispuesto por el artículo 9.2.b y 9.2.c en la disposición al penalizar "*toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales*".

c) Reserva al 9.1.e[128]: Se mantiene lo dispuesto por la normativa interna, en relación a que la posesión de material pornográfico infantil debe ir de la mano con la intención inequívoca de distribución o comercialización. Esta reserva es problemática al permitir implícitamente la posesión de material pornográfico infantil; que sumado a la reserva del 9.1.d y al silencio respecto de la adquisición de pornografía infantil, terminaría castigando sólo la oferta del material y no la demanda de este, lo que en este tipo de materias constituye una falencia regulatoria importante en consideración al bien jurídico protegido y al modo de operar del delito en cuestión.

d) Reserva al artículo 22.1. d[129]: Se reserva para no tener el deber de realizar la persecución penal contra nacionales en el extranjero que vulneren la ley del lugar en el que se encuentren al cometer el hecho. Se señala al efecto, que este punto contraría la definición de competencia penal internacional, lo que efectivamente crearía un sistema de jurisdicción penal distinto de

[127] "La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388".

[128] "La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL)".

[129] "La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional".

persecución penal internacional personal por infringir la ley territorial a pesar de que sea una conducta avalada por el país requerido.

e) Reserva al artículo 29.4[130]: Se señala que el artículo vulnera el principio de doble incriminación. Similar a la reserva anterior, se estima que se incumple con normas de competencia penal internacional. Del análisis de la disposición reservada se entiende que ratifica el principio; pero no en todos los casos, por lo que la reserva argentina se debe entender en sentido general.

d.- Estado de la normativa interna de adecuación del Convenio

Argentina no ha adoptado ni tiene en tramitación actualmente algún proyecto de ley de adecuación unificada de la normativa del Convenio de Budapest. Sin embargo, a la fecha se encuentran en tramitación proyectos relacionados en el Senado tales como el N°230/19 que modifica el Código Penal tipificando la publicación por medios informáticos de imágenes de personas en actividades sexuales y el robo de identidad, además del proyecto N°109/16 sobre utilización de programas informáticos de formato libre y el proyecto N°3918/14 sobre daño a un sistema informático. Por su parte, la Cámara de Diputados tiene en tramitación el proyecto de Ley 4199-D-2019 mediante el cual se establecería un agravante para los delitos cometidos a través de internet o por medios electrónicos.

Además, Argentina se encuentra tramitando el proyecto de Ley 2714-D-2017 que regula el agente encubierto informático[131], incorporándolo a las disposiciones de la Ley 27.319 sobre Delitos Complejos, definiendo agente informático online, en el artículo 2 del Proyecto como: *"Será considerado agente encubierto informático todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su*

[130] "La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL Nº24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados."

[131] DIPUTADOS ARGENTINA. Proyecto de Ley. 2017. [En línea] <https://www.hcdn.gob.ar/proyectos/proyecto.jsp?exp=2714-D-2017> [Consulta: 01 de julio de 2020]

identidad interactúe, se relacione o participe, a través de una identidad supuesta en grupos de internet, redes sociales y plataformas de intercomunicación on-line ,con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial".

El proyecto además contempla, la responsabilidad del agente policial, cómo deberá operar y forma de ejercer su encomienda; así, en el mensaje de fundamentos del Proyecto de Ley, se señala: *"Es por ello que el recurso de la tecnología por parte del Estado cumple en la actualidad un doble papel en relación con el proceso penal: por un lado permite el perfeccionamiento de los medios de análisis para investigación y prueba ofreciendo resultados más fiables, y por otro, permite la persecución de aquellos delitos conectados directamente con la tecnología, cada vez más numerosos."* El proyecto impulsado por la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), reconoce la masificación de los delitos vinculados a medios tecnológicos, y la utilización de ésta para la facilitación de su comisión, y como almacenamiento de evidencia esencial para el procesamiento de estos delitos.

3.- Uruguay.

a.- Contexto jurídico de ciberdelincuencia

En materia criminal el Código Penal uruguayo dispone en su artículo 277 bis la tipificación del contacto o influencia a menores de edad con intención de cometer delitos contra su integridad sexual por cualquier medio. Fuera de esta materia no hay regulación específica sobre delitos cometidos mediante medios informáticos. Cabe señalar que Uruguay tiene actualmente una regulación sobre la protección de datos personales mediante Ley 18.331 de 2008 que fue complementada por la Ley 19.670 de 2018 con el objetivo de reforzar las obligaciones y responsabilidad de los encargados de base de datos.

En materia procesal, Uruguay realizó una reforma mayor en el año 2017 mediante la Ley 19.293 de nuevo Código Procesal Penal, que estableció un sistema oral acusatorio, separando

las funciones de investigación y acusación de las funciones jurisdiccionales, dejando las primeras en el nuevo Ministerio Público. Este Código establece algunas medidas pertinentes al presente estudio: en su sección XIV "*de la interceptación e incautación postal y electrónica*"; en los artículos 205 y siguientes, consagra la facultad de solicitar judicialmente por parte del Ministerio Público la interceptación, incautación y apertura del correo electrónico o comunicaciones similares del imputado y la medida de intervención de comunicaciones (de contenido) en el artículo 209. En materia probatoria; además, se establece la filmación como medio de presentar el testimonio además de considerar al video dentro del concepto de documento[132].

b.- Etapa de implementación del Convenio de Budapest e hitos de su tramitación nacional

Uruguay no ha adherido al Convenio ni tampoco se encuentra tramitando legislativamente su incorporación.

4.- Colombia.

a.- Contexto jurídico de ciberdelincuencia

En Colombia ya existía una estructura normativa penal sobre delitos informáticos contenida en la Ley 1.273 de 2.009 "por medio de la cual se modifica el Código Penal un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"[133] que contiene una serie de delitos informáticos contemplados en el Convenio de Budapest[134] con especial atención a la protección de datos personales.

[132] Art. 175.3 del Código Procesal Penal uruguayo "Cuando el documento consista en un video, se ordenará su visualización y su transcripción en un acta, con intervención de las partes."

[133] COLOMBIA. Ministerio del Interior y Justicia. 2009. Ley 1273 de 2009. Enero, 2009. [En línea] <http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf.> [Consultado: 01.06.2020]

[134] Tipifica los siguientes delitos bajo el capítulo "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos": Acceso abusivo a un sistema informático; obstaculización ilegítima de sistema informático o red de telecomunicación; interceptación de datos informáticos; daño Informático; uso de software malicioso; violación de datos personales; suplantación de sitios web para capturar datos personales; además de establecer bajo el capítulo "De los atentados informáticos y otras infracciones" las figuras de hurto por medios informáticos y semejantes y transferencia no consentida de activos.

Respecto al derecho procesal penal el Código de Procedimiento Penal de Colombia, en su artículo 236 contiene la medida de "*recuperación de información dejada al navegar por internet u otros medios tecnológicos que produzcan efectos equivalentes*"[135] pero que se limita a la aprehensión física del *hardware* utilizado en el supuesto delito. Además, el decreto N°1.704 de 2012 regula la interceptación de comunicaciones y la obligación de los proveedores de servicios de internet de entregar a Fiscalía los datos del suscriptor (identidad, dirección, tipo de conexión) de forma inmediata debiendo mantener la información por un plazo de 5 años; además del deber de entregar información sobre la ubicación de dispositivos determinados.

b.- Etapa de implementación del Convenio de Budapest e hitos de su tramitación nacional

En el año 2013 el Ministerio de Relaciones Exteriores aceleró las gestiones para ser invitado a adherirse al Convenio[136], como parte de la política nacional de ciberseguridad[137]. En Colombia la aprobación de los tratados pasa por la firma del ejecutivo, la aprobación del Congreso y el control de constitucionalidad por parte de la Corte Constitucional. Con fecha 11 de septiembre de 2013 Colombia fue invitada a adherirse al instrumento con un plazo de 5 años para completar la tramitación interna, teniendo hasta el 12 de septiembre de 2020[138]. En junio de 2018 se aprobó la adhesión en Segundo Debate y en 24 de Julio se convirtió en Ley de la

[135] Art. 236: Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

[136] FUNDACIÓN KARISMA. Convenio de Budapest: Aplicación en Colombia frente a Derechos Humanos. 2018. Publicaciones Derechos Digitales. [En línea] <https://www.derechosdigitales.org/publicaciones/convenio-de-budapest-aplicacion-en-coombia-frente-a-derechos-humanos/> [Consulta: 01 de julio de 2020]

[137] Planteada mediante documento de Consejo Nacional de Política Social y Económica N°3701 de 2011.

[138] COUNCIL OF EUROPE, Treaty Office. 2019. Non-members States of the Council of Europe Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties. Status as of 26 august 2019. [En línea] <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22> [Consulta: 01 de junio 2020]

República N°1.928. A pesar de esto, no se ha formalizado el ingreso de Colombia ni sus reservas al Convenio de Budapest a la fecha del presente estudio[139].

c.- Declaraciones y reservas efectuadas al Convenio

Según lo dispuesto por el artículo 14 del Convenio, sobre disposiciones comunes, Colombia efectuó 2 reservas: una sobre el artículo 20 y otra sobre el artículo 21. Estas reservas consisten en limitar la aplicación de la medida de obtención en tiempo real de datos relativos al tráfico para que procesa solo respecto de delitos determinados. Sin embargo, no se señaló a qué delitos se limita la aplicación de tal medida, por lo que quedó una reserva sin aplicación concreta.

La otra reserva, sobre la interceptación de datos relativos al tráfico, se refiere a que la medida es procedente sólo en casos de que un sistema informático se haya puesto en funcionamiento para un grupo restringido de usuarios además de que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado.

d.- Estado de la normativa interna de adecuación del Convenio

Sin existir una adecuación legal específica sobre el Convenio ya aprobado, durante el año 2018 se promovieron 2 proyectos de ley relacionados a la regulación del cibercrimen, el proyecto de ley N°060/18 "*por medio de la cual se adoptan disposiciones de fortalecimiento de la seguridad ciudadana*" y el proyecto de ley N°074/18 "*por la cual se formulan los lineamientos de política pública para la prevención de delitos realizados a través de medios informáticos o electrónicos, en contra de niños, niñas y adolescentes, se modifica el código penal y se dictan otras disposiciones*". Ambos proyectos se encuentran acumulados en su tramitación[140] por

[139]COUNCIL OF EUROPE. 2004 Chart of signatures and ratifications of Treaty 185. [En línea] <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=I7GT616W> [Consulta: 01 de junio de 2020]

[140] GACETA DEL CONGRESO SENADO Y CÁMARA. Ponencias. Año XXVIII-N°349. Bogotá, D. C. Colombia, martes 14 de mayo de 2019.ISSN: 0123-9066. [En línea] <http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/Ponencias/2019/gaceta_349.pdf> [Consultado: 01 de julio de 2020]

decisión de la Mesa Directiva del Senado de la República y en su tercer capítulo regulan medidas contra la ciberdelincuencia y la cibercriminalidad que incluye la figura del *sexting*, uso de *software* malicioso, bloqueos de usuarios y dominios de internet.

Finalmente, del breve estudio realizado se evidencia la importancia que tiene la regulación penal y procesal penal en materias de cibercrimen, reconocida por la gran mayoría de los países y que ha posicionado al Convenio de Budapest más allá de los límites europeos como un buen modelo a seguir. La adhesión y adecuación (o modernización) normativa que se ha fomentado a raíz del Convenio contribuye a la consolidación de un modelo efectivo de investigación y persecución penal sobre delitos cometidos por medios informáticos en materias tan delicadas como la pornografía infantil, que requiere del mayor avance normativo junto con la cooperación internacional.

- Una materia para destacar es el foco que correctamente se ha puesto internacionalmente en materia de regulación sobre protección de datos personales, elemento sustancial para garantizar y compatibilizar la aplicación de las medidas del Convenio con el respeto a los derechos fundamentales de los ciudadanos, que en Chile se concentra en la Ley N° 19.628.

- Latinoamérica se encuentra atrasada en la tramitación del proyecto en general, existe una falta de adecuación y se evidencia que Chile se encuentra dando la discusión adecuada al respecto para darle plena vigencia a lo dispuesto por el tratado, mientras que Argentina, Uruguay y Colombia no han dado el paso a implementar la normativa. Esto se hace necesario toda vez que la Convención no es una norma autoejecutable; no tiene la pena para los delitos que establece; no cuenta con el detalle correspondiente a la legislación local correspondiente y en general señala una serie de obligaciones de “adecuar la legislación” que se encontrarían vacías si no se complementa la normativa.

- España se encuentra en un estado avanzado de reglamentación de medidas, incorporando disposiciones de mayor profundidad técnica como distintas vías de identificación del abonado respecto un dispositivo o viceversa; seguimiento y localización; agente encubierto en línea o registro remoto sobre equipos informáticos, ninguna de las cuales se encuentra en el Convenio de Budapest. Si bien resulta interesante este desarrollo normativo, se encuentra lejos de constituir un modelo a seguir. Esto porque las medidas estudiadas constituyen una grave afección de los derechos individuales y en muchos casos se ve un campo de aplicación muy amplio para permitir aquella intromisión.

- En relación con las reservas y declaraciones; Argentina evidencia un estudio más profundo y trabajado en lo que respecta a ciertas disposiciones de competencia penal internacional. Si bien nuestro país realizó reservas a su vez, no hubo pronunciamiento respecto de este tipo de materias, por lo que se podrían producir conflictos de competencia con nuestra normativa.

- Se denota una diversificación en la forma y oportunidad de la regulación; desde aquellos países que decidieron regular la materia en profundidad a propósito del Convenio, hasta aquellos que postergaron la ratificación para después de adecuar la normativa nacional (Colombia, Uruguay). También encontramos elementos comunes en la tramitación legislativa de los distintos marcos jurídicos, como lo son el diagnóstico compartido sobre las problemáticas jurídicas que conlleva la masificación del internet, en particular la preocupación respecto de los delitos contra la indemnidad sexual de menores, el sabotaje informático y la transferencia ilegítima de fondos millonarios (falsificación de tarjetas, *phishing*, *pharming*, etc).

CONCLUSIONES.

El desarrollo de la presente investigación nos permite determinar distintas conclusiones para los objetivos consignados al comienzo de este trabajo; y de la misma manera, otorga la posibilidad de plantear interrogantes sobre el futuro normativo contra la ciberdelincuencia:

Respecto de nuestro **objetivo principal**, consistente en analizar la respuesta a nivel nacional e internacional el fenómeno de la ciberdelincuencia; podemos concluir que siendo una problemática que afecta a todos los Estados, requiere necesariamente una respuesta coordinada y con estándares comunes mínimos para combatir los alcances internacionales y dinámicos de la ciberdelincuencia. Así, identificamos al Convenio de Budapest como la mayor respuesta en el campo internacional, con un alcance significativo en su aplicación y una elaborada estructura tanto procesal como sustantiva que reconoce a la cooperación internacional como uno de los pilares esenciales para su eficacia.

Este Convenio fue ambicioso en su origen; sin embargo, a 19 años de su suscripción, el Convenio se hace insuficiente para cubrir todos los aspectos actuales de la ciberdelincuencia, omitiendo regular figuras investigativas como el agente encubierto on-line. De esta manera, siendo una buena base, no exime a los Estados de la responsabilidad de complementar la materia para mantener sus legislaciones actualizada, frente al desarrollo constante de la tecnología.

En **específico,** en este punto, gracias al estudio de derecho comparado que nos entrega un mayor marco de análisis, comprobamos que en muchos casos; como en Chile, ha sido el Convenio la plataforma para discutir y modernizar la legislación ante la escasa regulación existente. Verificamos a su vez, que su contenido puede y debe ser adecuado por cada país adherente, lo que permite un amplio abanico de alternativas regulatorias según la realidad jurídica, donde se debe tener un especial cuidado con que tal adecuación se haga en pleno respeto de los derechos fundamentales, que se podrían ver fácilmente vulnerados si no se establecen límites concretos para las medidas intrusivas.

En particular, al analizar la estructura y herramientas del Convenio de Budapest; se puede señalar en primer lugar, la existencia de una gradualidad en las medidas intrusivas que llegan a extremos de interceptar en tiempo real el contenido de las comunicaciones de un imputado (artículo 21), lo que constituye una herramienta sumamente peligrosa para el respeto al derecho de privacidad de todo particular. Sin embargo, debido a los límites del Convenio, no quedan suficientemente regulados sus requisitos de procedencia. La única aprensión particular que el Convenio hace a su aplicación es que sea a "*un catálogo de delitos graves*" según la determinación de cada parte.

Por tanto, se deja toda la carga al Estado adherente para especificar la aplicación de las medidas más lesivas, con un mandato general de respetar tratados internacionales de derechos humanos que la misma parte haya suscrito. Esto conlleva una tremenda responsabilidad en la adecuación del Convenio, proceso en el cual se corre el riesgo de establecer medidas persecutorias absolutamente desproporcionadas, para lo que se requiere un adecuado estudio que ponga por delante los derechos fundamentales de todos los ciudadanos. En nuestro país tenemos experiencias sobre la utilización abusiva de estos métodos; como ocurrió en el caso Huracán, lo que hace especialmente preocupante la falta de exigencias y llama a seguir con atención su consagración legal interna.

Si bien, Chile fue invitado a adherir la Convención el año 2009, recién el 2016 se presenta el "Proyecto que aprueba el Convenio", desconocemos los motivos del retraso, considerando que el 2004 ya hubo estudios que fueron favorables a que Chile adhiriera al instrumento. De ello deducimos que Chile ha actuado con falta de prolijidad en el estudio del Convenio y sus implicancias; desconociendo su importancia ante la desactualización de la normativa interna que tenía como herramienta principal la Ley 19.233, proveniente del año 1993, la cual, si bien se había ocupado de tipificar los delitos informáticos, ha tenido una baja aplicación y no resuelve los actuales desafíos de la criminalidad informática.

A lo anterior se suma el aumento gradual de casos nacionales, y de requerimientos de cooperación internacional en la materia, que llevaron a que tanto la comunidad científica nacional como los organismos investigativos instaran su pronta aprobación.

Finalmente, el año 2016 se logra la ratificación del convenio, dando paso a la asistencia internacional en su implementación efectiva, sobre todo en lo que respecta a dotar a las policías de las herramientas que les permitiera mayor eficacia en las investigaciones en este tipo de delitos.

En cuanto a los objetivos específicos, a partir del análisis a fondo del proyecto de ley de adaptación del Convenio podemos señalar que se está en un buen camino gracias a la atención puesta sobre las observaciones de la academia y sociedad civil en el trabajo de las comisiones, lo que ha permitido mejorar el proyecto original mediante la aprobación de una serie de indicaciones. Sin embargo, se mantienen ciertos focos de preocupación en relación al estado actual del proyecto, tales como la responsabilidad en la tenencia y conservación prolongada de metadatos por entes privados con poca regulación efectiva; los contornos y requisitos específicos para solicitar judicialmente información de contenido de un imputado y el riesgo de vulnerar información de terceros ajenos a la investigación; o los límites del agente encubierto informático recientemente incorporado.

Finalmente, en cuanto a los desafíos futuros, a pesar de que actualmente han suscrito 62 países, la ausencia de importantes países, como los del bloque BRICS afecta la eficacia del Convenio, ya que impide aplicar un lenguaje común a sectores de la población mundial, debiendo recurrir a normas supletorias del derecho internacional público y tratados suscritos con aquellos Estados en particular.

Por otro lado, encontramos a la protección de datos personales como un desafío pendiente en materia internacional, lo que no ha sido foco de urgencia como lo fue la regulación sobre ciberdelincuencia hace ya más de 18 años. Actualmente existen lineamientos de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos actualizados en 2003 pero como un marco mínimo y no vinculante. Europa se encuentra más avanzada en esta materia,

mediante el Convenio 108 del Consejo (sucedido por el Reglamento General de Protección de Datos) y la Directiva 95/46/CE de la Unión Europea, sumado al reconocimiento explícito en el TFUE (artículo 16) y en la Carta de Derechos Fundamentales de la U.E. (artículo 8). Esto sin embargo no ha tenido la misma pretensión de universalidad, lo que ha generado conflictos en la asimetría del tratamiento de los datos y que llama a profundizar esta regulación fuera de los límites europeos, lo que debería ir de la mano con la discusión sobre medidas intrusivas en la red.

En Chile, se avizora la aprobación del proyecto de ley estudiado sin muchas modificaciones, toda vez ya fue trabajado y aprobado por unanimidad en el Senado. Ha servido para discutir sobre la protección de datos personales y la responsabilidad en la tenencia de éstos, incluso limitando el tiempo para su eliminación a 1 año según el actual proyecto de ley. Sin embargo, no se han aumentado los requisitos para las medidas restrictivas, las que incluso se ampliaron mediante la inclusión del agente encubierto en línea además de la separación de las medidas de acceso a información de suscripción y de tráfico, manteniendo la ausencia de requisitos que estén a la altura de la vulneración en relación con la entrega de información sobre contenido de comunicaciones. Es de esperar que la Cámara Revisora vaya puliendo estas omisiones, estableciendo exigencias elevadas para medidas de alta afectación individual.

Se volverá fundamental; por tanto, el baremo que se aplique mediante la primera salvaguarda interna: el control jurisdiccional. Y es que será esta instancia donde se realizarán los ejercicios de ponderación concretos que vayan limitando la aplicación excesiva de estas medidas, donde esperamos que se aplique un criterio conservador y restrictivo sobre las medidas, con pleno respeto de los derechos fundamentales de los imputados y de terceros que se podrían ver afectados.

BIBLIOGRAFÍA.

Artículos de revistas.

- AGUIRRE Romero, Joaquín. Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. Revista de estudios literarios; Espéculo, Biblioteca virtual universal, Universidad Complutense de Madrid; ISSN 1139-3637. España; octubre, 2004.

- ARAVENA Estrada, Eduardo. Conflictos de soberanía en la implementación del Convenio de Budapest: análisis crítico de la conservación y acceso transfronterizo de datos personales para la persecución internacional de ciberdelitos. 5to simposio internacional LAVITS Vigilancia, democracia y privacidad en América Latina: Vulnerabilidades y resistencias. ISSN 2175-9596, pp 322-336. Santiago, Chile; noviembre, 2017.

- ARMENTA Deu, Teresa. Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre. Revista de los Estudios de Derecho y Ciencia Política; IDP N.º 27. ISSN 1699-8154, pp 67-79. España; septiembre, 2018.

- ARNOLD, Rainer; MARTÍNEZ Estay, José Ignacio y ZÚÑIGA Urbina, Francisco. El Principio De Proporcionalidad En La Jurisprudencia Del Tribunal Constitucional. Estudios constitucionales, año 10; N° 1, Centro de Estudios Constitucionales de Chile Universidad de Talca. ISSN 0718-0195, pp 65-116. Chile, 2012.

- BARNES, Javier. Introducción al principio de Proporcionalidad en el Derecho comparado y comunitario. Revista de Administración Pública, N°135. ISSN 0034-7639, pp 495- 522. España, 1994.

- BRENNER, Susan. La Convención sobre Cibercrimen del Consejo de Europa. Revista chilena de Derecho y Tecnología; Universidad de Chile, Volumen I, Nro. I. ISSN 0719-2576, pp 221- 238. Chile, 2012.

- BORGES Blázquez, Raquel. La prueba electrónica en el proceso penal y el valor probatorio de conversaciones mantenidas utilizando programas de mensajería instantánea. Revista Boliviana de Derecho, N°25. ISSN 2070-8157, pp 536-549. Bolivia; enero, 2018.

- BOSCH Cartagena, Camila. Evidencia Digital. El Convenio de Budapest y sus desafíos en el Derechos Procesal Penal. Revista Jurídica Ministerio Público N°72. ISSN 0718-6479, pp 121-141. Santiago, Chile; abril, 2018.

- DÍAZ Gómez, Andrés. El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de La Rioja, REDUR, ISSN 1695-078X, pp 169-203. España; diciembre, 2010.

- ESTRADA, Rodolfo; Somellera, Roberto. Delitos informáticos. Informática y derecho: Revista iberoamericana de derecho informático, ISSN 1136-288X, pp 423- 442. México; 1998.

- FERNÁNDEZ Rodríguez, J. J. Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente. Revista Española de Derecho Constitucional, N°108. ISSN 0211-5743, pp 93-122. España; diciembre, 2016.

- GILLES Bélanger, Pierre. Derechos Humanos y el derecho penal en el ciberespacio. Revista Secretaria Tribunal permanente de revisión, Mercosur; Año 5, Nº10. ISSN 2304-7887, pp 274 - 286. Octubre, 2017.

- HERNÁNDEZ Basualto, Héctor. Uso indebido de tarjetas falsificadas o sustraídas y de sus claves. Revista Política Criminal; N°5, volumen 3. ISSN 0718-3399, pp 1-38 (A2- 5). Talca, Chile; julio, 2008.

- LÓPEZ-BARAJAS Perea, Inmaculada. Nuevas tecnologías aplicadas a la investigación penal: el registro de equipos informáticos. Revista de Internet, Derecho y Política. ISSN 1699-8154, pp 64-76. Cataluña, España; mayo, 2017.

- MARÍN, Juan Carlos; GARCÍA, Guillermo. Problemas que enfrenta la prueba digital en los Estados Unidos de Norteamérica. Revista de Estudios de Justicia, N°21. ISSN 0718-0853, pp 75- 91. Santiago, Chile; marzo, 2015.

- MONTENEGRO Torres, María Luisa. Cooperación internacional: tramitación, obtención de pruebas e incorporación de documentos y evidencias. Revista Jurídica Ministerio Público N°70. ISSN 0718-6479, pp 63- 85. Santiago, Chile; agosto, 2017.

- RAYMAN Labrín, Danny. Chile: Vigilancia y derecho a la privacidad en internet. Revista Chilena de Derecho y Tecnología; Centro de Estudios en Derecho Informático, Universidad de Chile. Vol. 4, Número 1. ISSN 0719-2576, pp 187-232. Santiago, Chile; 2015.

- SEGOVIA Arancibia, Antonio Los equipos conjuntos de investigación como herramienta de Cooperación Internacional. Revista Jurídica Ministerio Público N°72. ISSN 0718-6479, pp 69-95. Santiago, Chile; abril, 2018.

Tesis.

- GUIÑEZ Navarro, Paz. Decreto N° 866 sobre interceptación de las comunicaciones telefónicas y de otras formas de telecomunicación y de conservación de datos comunicacionales, a la luz de la normativa constitucional. Tesina de Magíster, Universidad Finis Terrae. 2018.

- MATEOS Pascual, Iván. Ciberdelincuencia, desarrollo y persecución tecnológica. Proyecto Fin de Carrera E.U.I.T. Telecomunicación (UPM). Universidad politécnica Madrid. 2013.

- MERINO García, Felipe. Delitos informáticos y las salidas alternativas posibles revisadas desde el análisis económico del derecho. Memoria para optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales. Universidad de Chile, Departamento Derecho Procesal. Santiago, Chile. 2017.

- SÁNCHEZ Hernández, José. Estudio de la prueba electrónica en el proceso penal: especial referencia a las conversaciones de whatsapp. Trabajo fin de Título, Máster en acceso a la abogacía Materia: Orden Jurisdiccional Penal, Universidad de Salamanca, España. 2017.

- VALDIVIESO Villanueva. Laura, Las diligencias de investigación tecnológica y su aplicación práctica en el Orden Jurisdiccional Penal. TFM. Universidad de Salamanca. 2016.

Otros.

- ARGENTINA. Proyecto de Ley, Modificaciones sobre incorporación de la figura de agente encubierto informático. Delitos complejos Ley 27.319 [En línea] <https://www.hcdn.gob.ar/proyectos/proyecto.jsp?exp=2714-D-2017> [consulta: 01 de julio de 2020]

- BOLETÍN Oficial del Estado Número 239, páginas 90220 a 90239. BOE A-2015-10726. [En línea] <https://www.boe.es/eli/es/l/2015/10/05/41> [consulta: 01 de julio de 2020]

- CENTENO, Danya. México y el Convenio de Budapest, posibles incompatibilidades. Publicaciones Derechos Digitales, junio 2018. [En línea]

<https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 01 de julio de 2020]

- CHAHUÁN Sarrás, Sabas. Manual del Nuevo Procedimiento Penal. Thomson Reuters, séptima edición. 2012. ISBN 978-956-346-103-9
- CHILE. Constitución Política de la República.
- CHILE. Ley General de Telecomunicaciones, número 18.168, Ministerio de Transporte y Telecomunicaciones, 1982. Última versión: agosto 2019 [En línea] <http://bcn.cl/2b8s6> [consulta: 01 de julio de 2020]
- COLOMBIA. Código Penal colombiano [en línea] <http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf> [consulta: 01 de julio de 2020]
- CONSEJO de Europa. Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime Status. [En línea] <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ef9Uje9G> [consulta: 01 de julio de 2020]
- CONSEJO de Europa. Explanatory report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed though computer systems. Estrasburgo, 2013. [En línea] <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f> [consulta: 01 de julio de 2020]
- CONSEJO de Europa. Informe Explicativo Budapest. [En línea] <https://rm.coe.int/16802fa403> [consulta: 01 de julio de 2020]

- CONSEJO de Europa. Convención sobre Ciberdelincuencia. [En línea] <http://bcn.cl/21t2c> [consulta: 01 de julio de 2020]
- Convención Europea de Asistencia Mutua en Materia Penal, suscrita en Estrasburgo, el 20 de abril de 1959. [En línea] <http://bcn.cl/213ec> [consulta: 01 de julio de 2020]
- CONSEJO de Europa, Treaty Office. "Non-members States of the Council of Europe Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties". [En línea] <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22> [consulta: 01 de julio de 2020]
- CONSEJO de Europa. Mutual Legal Assistance Manual. Belgrado, Serbia. ISBN 978-86-84437-57-2. 2013. [En línea] <https://rm.coe.int/mutual-legal-assistance-manual-eng/1680782927> [consulta: 01 de julio de 2020]
- CONTRALORÍA General de la República. Dictamen N°41.188-17. [En línea] <https://www.contraloria.cl/pdfbuscador/dictamenes/041188N17/html> [consulta: 01 de julio de 2020]
- ESPAÑA. Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. [En línea] <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036> [consulta: 01 de julio de 2020]
- ESTADOS UNIDOS. 18 US Code. § 1.030. Fraud and related activity in connection with computers. [En línea] <http://bcn.cl/1nmu1> [consulta: 01 de julio de 2020]
- FUNDACIÓN KARISMA. Convenio de Budapest: Aplicación en Colombia frente a Derechos Humanos. Publicaciones Derechos Digitales, junio 2018. [En línea] <https://www.derechosdigitales.org/publicaciones/convenio-de-budapest-

aplicacion-en-coombia-frente-a-derechos-humanos/> [consulta: 01 de julio de 2020]

- GARAY, Vladimir y ROGOFF, Zak. Tecnología y vigilancia en la operación huracán: una revisión del trabajo periodístico realizado en torno al caso. Publicaciones Derechos Digitales; septiembre, 2018. [En línea] <https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 01 de julio de 2020]

- GUERRERO Argote, Carlos. De Budapest al Perú: Análisis sobre el proceso de implementación del Convenio de Ciberdelincuencia. Impacto en el corto, mediano y largo plazo. Publicaciones Derechos Digitales, junio 2018. [En línea] <https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 01 de julio de 2020]

- INTERPOL. Estrategia mundial contra la Ciberdelincuencia. Febrero 2017. [En línea] <https://www.interpol.int/ar/content/download/5586/file/Summary_CYBER_Strategy_2017_01_SP%20LR.pdf?inLanguage=esl-ES> [consulta: 01 de julio de 2020]

- MINISTERIO Público de Chile. Instrucciones Generales, Facultades Autónomas, Primeras Diligencias, Artículos 83 y 87 Código Procesal Penal. Actualización septiembre de 2017.

- MINISTERIO de Transporte y Telecomunicaciones. Resolución exenta 1.483, de 22 de octubre de 1999 que fija el procedimiento y plazo para establecer y aceptar interconexiones entre Proveedores. [En línea] <http://bcn.cl/269ux> [consulta: 01 de julio de 2020]

- NACIONES UNIDAS, oficina contra la droga y el delito. Delincuencia organizada transnacional - La economía ilegal mundializada. [En línea] <https://www.unodc.org/documents/toc/factsheets/TOC12_fs_general_ES_HIRES.pdf> [consulta: 01 de julio de 2020].

- PINACCHIO, María Clara, Ángela. Los desafíos que las tecnologías plantean incorporarse a los procesos judiciales. 17 de octubre de 2017. [En línea] <www.saij.gob.ar.> ID: DACF170419. [consulta: 01 de julio de 2020]

- RIVOLTA, Mercedes. Medios de prueba electrónicos: estado de avance en la legislación argentina. Sistema Argentino de Información Jurídica 2007. [En línea] <www.saij.jus.goc.ar> ID: DACC070049. [consulta: 01 de julio de 2020]

- SENADO. Informe de la Comisión de Relaciones Exteriores, recaído en el proyecto de acuerdo, en segundo trámite constitucional, que aprueba el "Convenio sobre la Ciberdelincuencia, suscrito en Budapest, Hungría, el 23 de noviembre de 2001." BOLETÍN Nº10.682-10.

- SEQUERA, Maricarmen. SAMANIEGO, Marlene. Cibercrimen: Desafíos de la armonización de la Convención de Budapest al Sistema Penal paraguayo. Publicaciones Derechos Digitales, junio 2018. <https://www.derechosdigitales.org/tipo_publicacion/publicaciones/> [consulta: 01 de julio de 2020]

- URUGUAY. Código Procesal Penal [En línea] <https://www.impo.com.uy/bases/codigo-proceso-penal-2017/19293-2014> [consulta: 01 de julio de 2020]