**UNIVERSIDAD DE SANTIAGO DE CHILE**

**FACULTAD DE INGENIERÍA**

**DEPARTAMENTO DE INGENIERÍA INFORMÁTICA**

**MAGÍSTER EN SEGURIDAD, PERITAJE Y AUDITORÍA EN PROCESOS**

**INFORMÁTICOS**

ESTUDIO COMPARATIVO DE LA LEGISLACIÓN CHILENA SOBRE DELITOS INFORMÁTICOS Y EL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA

**VÍCTOR ARMANDO SERRANO VERDUGO**

Profesor guía: Juan Ignacio Iturbe Araya

Trabajo de graduación presentado en conformidad a los requisitos para obtener el grado de Magister en Seguridad, Peritaje y Auditoría en Procesos Informáticos

Santiago, Chile

2017

**© Víctor Armando Serrano Verdugo, 2017**

 • Algunos derechos reservados. Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-Compartir Igual 3.0. Sus condiciones de uso pueden ser revisadas en: <<http://creativecommons.org/licenses/by-nc-sa/3.0/cl/>>

**RESUMEN**

El presente estudio tiene como finalidad analizar la problemática que ha causado la desactualización de la ley de delitos informáticos chilena y la posible adherencia al Convenio de Budapest sobre la ciberdelincuencia. De acuerdo a lo expresado anteriormente, en Chile se aprecia la carencia de una ley para combatir los ciberdelitos, la que se encuentre actualizada y sea acorde a los tiempos modernos. Hoy en día Chile tiene dos escenarios para solventar esta necesidad, el primero de ellos es concretar la adherencia al tratado de Budapest o llevar a cabo una actualización de la actual ley y el segundo, se podría ver enfrentado con trabas constitucionales, las que podrían poner en riesgo la adhesión a este tratado.

Dicho lo anterior, se recurrió a la recopilación de información mediante consultas por la ley de transparencia ciudadana y la lectura de documentos sobre la materia. Junto con lo anterior, se realizó un estudio comparativo de legislaciones vigentes de distintos países de Latinoamérica, que tuvieran contemplado dentro de su régimen los delitos informáticos. Otro punto importante llevado a cabo para la presente investigación, fue el desarrollo de casos de juicios desarrollados en Chile por infringir la Ley N° 19.223, se plantearon en conformidad de los artículos del Convenio de Budapest.

Con el desarrollo del estudio, se obtuvieron ventajas y desventajas de las soluciones propuestas. En la realización de la investigación se evidenció una de las dificultades a las que se podrá ver expuesto el proyecto de ley que habla sobre la futura adhesión al Convenio de Budapest. Esta opción se contrasta con el análisis de los proyectos de ley desarrollados para actualizar la ley de delitos informáticos. Bajo estos resultados obtenidos, se ha podido deducir cual puede ser la opción para Chile para dar una solución concreta para combatir los delitos informáticos. Sin embargo, junto con lo anterior, también se ha recomendado una serie de medidas las cuales serán de gran ayuda para dar un mejor entendimiento a la ciudadanía y al nivel de poder judicial y legislativo.

Palabras clave: Convenio de Budapest sobre la ciberdelincuencia, delitos informáticos, poder judicial y legislativo.

**ABSTRACT**

The purpose of this study is to analyze the problems caused by the outdated Chilean cybercrime law and the possible adherence to the Budapest Convention on Cybercrime. According to the above, in Chile we can appreciate the lack of a law to combat cybercrime, which is up to date and in keeping with modern times. Nowadays Chile has two scenarios to solve this need, the first one is to concretize adherence to the Budapest treaty or to carry out an update of the current law and the second, could be faced with constitutional obstacles, which could put Accession to this treaty.

That said, we used the collection of information through consultations by the law on citizen transparency and the reading of documents on the subject. Along with the above, a comparative study of current legislation of different countries of Latin America was carried out, which included computer crimes within its regime. Another important point made for the present investigation was the development of cases of trials developed in Chile for violation of Law No. 19,223, which were brought in conformity with the articles of the Budapest Convention.

With the development of the study, advantages and disadvantages of the proposed solutions were obtained. In carrying out the research, one of the difficulties that the draft law on the future accession to the Budapest Convention will be exposed will be shown. This option is contrasted with the analysis of the bills developed to update the computer crime law. Under these results, it has been possible to deduce what may be the option for Chile to give a concrete solution to combat computer crimes. However, along with the above, a number of measures have also been recommended which will be of great help in providing a better understanding of citizenship and the level of judicial and legislative power.

Key words: Budapest Convention on Cybercrime, Computer Crimes, Judicial and Legislative Branch.

**DEDICATORIA**

Para ustedes esposa, hijos y papá.

“Nunca dejes que nadie te diga que no puedes hacer algo”

**AGRADECIMIENTOS**

Gracias primero a Dios, por darme la fuerza y la paciencia, por abrirme los ojos para salir adelante cuando veía todo borroso y sin salida, me diste una luz de esperanza para continuar adelante.

A mi esposa Paola e hijos Lucas, Cristóbal y Amanda, muchas gracias por haber estado conmigo, por darme fuerzas y entusiasmo para salir adelante y lograr realizar este proyecto.

A mi papá, por ser un gran apoyo y enseñarme que con esfuerzo y paciencia todo se logra en la vida.

A mi profesor guía, Sr. Juan Iturbe, quien ha sido una persona que ha tenido una paciencia única conmigo y por no perder esa chispa de luz en mí para salir adelante.

Gracias a todos aquellos autores, que me ayudaron con sus artículos y libros.

**TABLA DE CONTENIDO**

[CAPÍTULO 1. INTRODUCCIÓN 1](#_Toc492026475)

[1.1. ANTECEDENTES Y MOTIVACIÓN 1](#_Toc492026476)

[1.2. DESCRIPCIÓN DEL PROBLEMA 3](#_Toc492026477)

[1.2.1. Dominio del problema 3](#_Toc492026478)

[1.2.2. Enunciado del problema 4](#_Toc492026479)

[1.3. SOLUCIÓN PROPUESTA 5](#_Toc492026480)

[1.3.1. Características de la solución 5](#_Toc492026481)

[1.3.2. Propósito de la solución 6](#_Toc492026482)

[1.4. OBJETIVOS Y ALCANCES DEL PROYECTO 7](#_Toc492026483)

[1.4.1. Objetivo general 7](#_Toc492026484)

[1.4.2. Objetivos específicos 7](#_Toc492026485)

[1.4.3. Alcances 8](#_Toc492026486)

[1.4.4. Limitaciones 8](#_Toc492026487)

[1.5. METODOLOGÍAS Y HERRAMIENTAS UTILIZADAS 8](#_Toc492026488)

[1.5.1. Metodología a usar 8](#_Toc492026489)

[1.5.2. Herramientas de desarrollo 9](#_Toc492026490)

[1.6. ORGANIZACIÓN DEL DOCUMENTO 10](#_Toc492026491)

[CAPÍTULO 2. REVISIÓN CRÍTICA DEL ESTADO DEL ARTE 12](#_Toc492026492)

[2.1 Ciberdelincuencia 12](#_Toc492026493)

[2.2 Convenio de Budapest sobre la Ciberdelincuencia 14](#_Toc492026494)

[2.3 Ciberdelitos en Chile 17](#_Toc492026495)

[2.4 Decreto N° 3265, crea comité interministerial sobre ciberseguridad 17](#_Toc492026496)

[2.5 Proyectos de modificación ley N° 19.223 de delitos informáticos 18](#_Toc492026497)

[2.6 Postura de Chile ante el Convenio de Budapest 21](#_Toc492026498)

[CAPÍTULO 3. ESTUDIO COMPARATIVO 23](#_Toc492026499)

[3.1. ESTUDIO COMPARATIVO 23](#_Toc492026500)

[3.1.1. Argentina 23](#_Toc492026501)

[3.1.2. Brasil 24](#_Toc492026502)

[3.1.3. Chile 24](#_Toc492026503)

[3.1.4. Colombia 25](#_Toc492026504)

[3.1.5. Perú 25](#_Toc492026505)

[3.1.6. Puerto Rico 26](#_Toc492026506)

[3.1.7. República Dominicana 27](#_Toc492026507)

[3.1.8. Uruguay 27](#_Toc492026508)

[3.1.9. Venezuela 28](#_Toc492026509)

[3.1.10. Tipificaciones de delitos informáticos según evaluación 28](#_Toc492026510)

[3.2. CONCLUSIONES 31](#_Toc492026511)

[CAPÍTULO 4. LEGISLACIÓN CHILENA 31](#_Toc492026512)

[4.1 LEGISLACIÓN CHILENA CONTENIDA EN CONVENIO DE BUDAPEST 32](#_Toc492026513)

[4.2 DERECHOS FUNDAMENTALES 33](#_Toc492026514)

[4.3 LEY DE TRANSPARENCIA 33](#_Toc492026515)

[4.3.1 Estadísticas de delitos informáticos 34](#_Toc492026516)

[4.3.2 Formalizaciones Delitos Informáticos 34](#_Toc492026517)

[4.4 CASOS DE ESTUDIO 40](#_Toc492026518)

[4.4.1 Hipermercado Curicó Ltda. con Lizama Ponce, María de las Nieves 40](#_Toc492026519)

[4.4.2 Sky Chile CPA con Merino Moraga, Pablo Andrés. 41](#_Toc492026520)

[4.4.3 Polincay Export y Comercial Polincay Ltda. con Pérez Rodríguez 42](#_Toc492026521)

[4.5 CONVENIO DE BUDAPEST EN CASOS APLICADOS 43](#_Toc492026522)

[4.5.1 Convenio de Budapest e hipermercado Curicó 44](#_Toc492026523)

[4.5.2 Convenio de Budapest y Sky Chile 45](#_Toc492026524)

[4.6 CONCLUSIONES 46](#_Toc492026525)

[CAPÍTULO 5. EVALUACIÓN Y ANÁLISIS DE RESULTADOS 47](#_Toc492026526)

[5.1 CONSTITUCIÓN DE CHILE Y EL TRATADO 48](#_Toc492026527)

[5.2 CAPACIDAD DE JUZGAR BAJO UNA LEY SIN CONOCIMIENTO 49](#_Toc492026528)

[CONCLUSIONES 51](#_Toc492026529)

[CONCLUSIONES GENERALES 52](#_Toc492026530)

[CUMPLIMIENTO DE LOS OBJETIVOS 53](#_Toc492026531)

[TRABAJOS FUTUROS 55](#_Toc492026532)

[REFERENCIAS BIBLIOGRÁFICAS 56](#_Toc492026533)

[ANEXOS 61](#_Toc492026534)

**ÍNDICE DE TABLAS**

Tablas del Capítulo 1

[Tabla 1.1 Actividad Maliciosa. Fuente: Clasificación General - América 2011, Symantec 3](#_Toc492039015)

Tablas del Capítulo 2

[Tabla 2.1 Proyectos de modificación Ley 19.223. Fuente: Elaboración propia (2016) 19](#_Toc492039016)

Tablas del Capítulo 3

[Tabla 3.1 Delitos contenidos en legislaciones de países analizados. Fuente: Elaboración propia (2016). 29](#_Toc492039017)

Tablas del Capítulo 4

[Tabla 4.1 Leyes influenciadas por las tecnologías de la información. Fuente: Elaboración propia (2016) 32](#_Toc492039018)

[Tabla 4.2 Cantidad de delitos que han sido investigados por la Policía de Investigaciones de Chile. Fuente: Elaboración propia (2016) 34](#_Toc492039019)

[Tabla 4.3 Detenidos por infracción a la Ley 19.223 por la Policía de Investigaciones de Chile. Fuente: Elaboración propia (2016) 35](#_Toc492039020)

**ÍNDICE DE ILUSTRACIONES**

Figuras del Capítulo 4

Figura 4.1 Delitos informáticos período 2010 a 2015. Fuente: Elaboración propia (2016) 35

Figura 4.2 Delitos investigados por infracción a la Ley N° 19.223 periodo 2010 a 2015. Fuente: Elaboración propia (2016) 36

Figura 4.3 Delitos puestos a disposición e investigados 2010 a 2015. Fuente: Elaboración propia (2016) 37

Figura 4.4 Delitos puestos a disposición de tribunales por infracción a la Ley N° 19.223 periodo 2010 a 2015. Fuente: Elaboración propia (2016) 38

Figura 4.5 Espionaje Informático a nivel nacional comprendido entre 2010 – 2015. Fuente: Elaboración propia (2016) 39

Figura 4.6 Sabotaje Informático a nivel nacional comprendido entre 2010 – 2015. Fuente: Elaboración propia (2016) 40

# INTRODUCCIÓN

## ANTECEDENTES Y MOTIVACIÓN

El avance de las tecnologías de la información y comunicación han revolucionado la vida de la sociedad en numerosos aspectos: científicos, laborales, profesionales, escolares, entre otros. Este progreso ha provocado un cambio en los hábitos de entretenimiento, relaciones familiares y sociales de los individuos, como por ejemplo la introducción de las redes sociales como *Facebook*, *Twitter*, por nombrar algunos

El sistema legal chileno en materia de delitos informáticos, se ha visto enfrentado a la incapacidad de actualizarse a la misma velocidad que las tecnologías lo realizan. Esta limitación se traduce en un impedimento en la regulación de los fenómenos o actos que utilicen las tecnologías de información para cometer ilícitos que violentan los sistemas informáticos.

En Chile, la Ley Nº 19.223 de delitos informáticos, promulgada en el año 1993, contempla cuatro artículos. Cada uno de ellos corresponde a un tipo de conducta distinta entre sí, pudiendo ser clasificadas en dos figuras delictivas; *sabotaje y espionaje informático.* Esta ley, fue desarrollada cuando las tecnologías y el uso de internet no eran un bien que toda la población nacional pudiera acceder. Sin embargo, con la promulgación de esta normativa, Chile pasó a ser pionero en la región latinoamericana al tipificar sobre este tipo de actos ilícitos. A continuación se describen los artículos de la citada ley que tipifican los delitos informáticos:

* + - *“Artículo 1°. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.*

*Si como consecuencia de estas conductas, se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo”.* (Nacional, 1993)

* + - *“Artículo 2°. El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio”.* (Nacional, 1993)
    - *“Artículo 3°. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio”.* (Nacional, 1993)
    - *“Artículo 4°. El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio.*

*Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”.* (Nacional, 1993)

La Ley N° 19.223 de delitos informáticos, describe las figuras penales de sabotaje y espionaje informático. Ahora bien, el sabotaje informático (artículos 1 y 3 de la presente ley), comprende las conductas que interfieren con el correcto funcionamiento de los componentes (*hardware o software*) con los cuales se encuentra desarrollado el sistema de tratamiento de información. Junto con lo anterior también se encuentran contemplados los datos contenidos en el sistema automatizado de tratamiento de la información. Dentro de las conductas que se encuentran descritas como acciones interferentes en el funcionamiento del sistema de tratamiento de información, se encuentra la destrucción, inutilización, obstaculización o modificación de los componentes y/o los datos (Informatico, 2014). Siguiendo con las conductas sancionadas por la ley de delitos informáticos, encontramos también la figura de espionaje informático (artículo 2 y 4 de la presente ley), que comprende las figuras delictivas relacionadas con el apoderamiento indebido (apropiarse de la información), uso indebido, es decir, usar la información para cualquier fin o conocimiento ilícito de la información, interfiriendo o interceptando o meramente accediendo al sistema de tratamiento de datos. Por último, cabe señalar que también se encuentran comprendidos los delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información (artículo 4º de la ley) (Informatico, 2014).

De acuerdo a lo anterior, la normativa chilena de delitos informáticos, no contempla los actos que están relacionados con el *phishing*, *malware* o el *hackeo* de páginas web (Symantec O. , 2014). Estas acciones ilícitas, son consecuencia de un acelerado crecimiento global de las tecnologías de información. A raíz de estas acciones la empresa Symantec, reconocido fabricante software a nivel mundial, generó el “*Informe Sobre Amenazas a la Seguridad en Internet*” (Symantec, 2012), en donde evaluó a los países de la región de América (que incluye Norteamérica y Latinoamérica), siendo esta última, la que concentra la mayor cantidad de actividad maliciosa a nivel mundial. Mediante la evaluación llevada a cabo por Symantec, Chile se posiciona en quinto lugar entre los países que más amenazas genera en la región. En la Tabla 1.1, se visualizan los países que han sido evaluados por la generación de actividades maliciosas evaluadas.

Tabla 1.1 Actividad Maliciosa. Fuente: Clasificación General - América 2011, Symantec

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| País | Ranking regional 2011 | Ranking mundial 2011 | Código Malicioso | Zombies de Spam | Phishing | Ataques Web por País |
| Brasil | 1 | 4 | 1 | 1 | 1 | 1 |
| Argentina | 2 | 22 | 5 | 2 | 3 | 4 |
| Colombia | 3 | 28 | 3 | 5 | 2 | 5 |
| México | 4 | 29 | 2 | 7 | 5 | 2 |
| Chile | 5 | 34 | 4 | 4 | 4 | 3 |
| Perú | 6 | 41 | 7 | 3 | 10 | 11 |
| Venezuela | 7 | 11 | 6 | 9 | 9 | 6 |
| República Dominicana | 8 | 54 | 9 | 6 | 25 | 15 |
| Uruguay | 9 | 61 | 20 | 8 | 15 | 9 |
| Puerto Rico | 10 | 73 | 11 | 17 | 20 | 13 |

Ahora bien, de acuerdo a lo observado en la Tabla 1.1, la falta de una normativa actualizada que vele por el comportamiento de la sociedad en la utilización de las tecnologías de la información pone a Chile en el quinto lugar en la región en producción de actividades maliciosas. De acuerdo a lo anterior, se puede deducir que la falta de control sobre estos actos, se debe a la carencia de una regulación que mantenga estas actividades controladas y reguladas. Actualmente la situación legal de Chile, o sea, la legislación nacional de delitos informáticos, se encuentra desactualizada, lo que hace pensar en la adopción de un tratado internacional que norme este tipo de actos o la una modificación a la normativa actual, la que debería ser acorde a los tiempos modernos, es decir, deberá brindar de ayuda a la sociedad a defenderse de los actos maliciosos que se desarrollan con el uso de las tecnologías de la información.

## DESCRIPCIÓN DEL PROBLEMA

### Dominio del problema

Durante el año 2001 se realizó en Budapest, Hungría, el congreso sobre la ciberdelincuencia, el que fue convocado por el Consejo de Europa (Europe, 2001). Este congreso dio origen al desarrollo de un tratado internacional, conocido como Convenio de Budapest, que sería utilizado para desarrollar medidas para enfrentar el cibercrimen. Este tratado ha sido aceptado por 47 Estados (ver Anexo A), incluidos los 28 Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia, Japón, Sudáfrica y República Dominicana (Europe, 2001).

El Convenio de Budapest sobre la Ciberdelincuencia (Europe, 2001), establece la necesidad de normar sobre el correcto uso y el desarrollo de las tecnologías de información entre los países que se han adherido al tratado. La normalización de las conductas es llevada a cabo mediante el establecimiento de medidas que previenen los actos maliciosos sobre los sistemas informáticos y de las tecnologías de la información, que puedan atentar contra la disponibilidad, confidencialidad e integridad de los datos que utilizan estas tecnologías. Las medidas descritas en el tratado, buscan evitar el abuso de sistemas, redes y datos. Estas ordenanzas descritas en el convenio, son desarrolladas mediante la utilización de herramientas y métodos que otorgan facultades para la investigación y la sanción, lo que es llevado a cabo por medio de acciones de mutuo acuerdo de cooperación entre los países adheridos al convenio. Por otra parte el tratado insta a la adopción de técnicas intrusivas de investigación, conservación de evidencia para combatir delitos cometidos mediante el uso de sistemas informáticos y el de colaboración entre los Estados miembros adheridos al convenio (Europe, 2001).

Por su parte Chile, cuenta con la opción de realizar la adhesión al Convenio de Budapest sobre la Ciberdelincuencia o la de realizar una modificación a la actual Ley N° 19.223 de Delitos Informáticos. Estas opciones descritas, implicarían para el poder legislativo adoptar y desarrollar nuevas figuras penales para los nuevos ilícitos que vulneran la seguridad de la información de los usuarios por medio de los sistemas de información.

En Chile, durante el año 2009, por medio del Decreto Supremo N° 3265 (Interior, 2009), se crea la Comisión Interministerial Conducente a la Adhesión de Chile a la Convención sobre Ciberdelitos del Consejo de Europa. La finalidad de este comité fue la de evaluar la adhesión al tratado por parte de Chile. Durante el año 2015, se dicta el Decreto Supremo N° 533 (Pública, 2015), con el que se retoman las conversaciones sobre la creación de la Comisión, teniendo como principal objetivo el crear una política nacional de ciberseguridad, que resguarde la imagen, dignidad y honor de las personas; combata la propagación de material que transgreda su intimidad; y que sea implacable al perseguir delitos relacionados con la pornografía infantil.

### Enunciado del problema

El sistema legal chileno en términos de delitos informáticos, no se encuentra actualizado. Esta falta de renovación a la Ley N° 19.223 de delitos informáticos, se debe al ritmo agitado del avance de las tecnologías de información, traduciéndose en un impedimento en la regulación fenómenos o conductas ilícitas que atentan contra la sociedad por medio de las tecnologías. Como consecuencia de esta situación las personas y las organizaciones de la sociedad chilena se ven desprotegidas, muchas veces dañadas y obligadas a resguardarse sin el apoyo legal adecuado para la regulación de estas conductas atípicas que han surgido. De acuerdo a la problemática expresada anteriormente, se formularon las siguientes interrogantes con las cuales se definió la problemática actual de Chile en materia de delitos informáticos:

* ¿Qué hacer para contribuir a la regulación de la conducta de las personas que realizan actos maliciosos a través de las tecnologías de la información con el fin de mejorar y/o sancionar las condiciones de seguridad humana de la sociedad chilena frente a estas amenazas?
* ¿Cuál es la brecha de la legislación actual chilena en cuanto a delitos informáticos y la legislación en este tema mundialmente aceptada?
* ¿Cuáles serán los impactos sobre la confidencialidad de los datos de los usuarios chilenos si se llevase a cabo la adherencia al Convenio de Budapest sobre la Ciberdelincuencia y la de actualizar la actual Ley N° 19.223 de delitos informáticos tipificando las nuevas conductas que son sinónimo del avance de las tecnologías?
* ¿Cuál es la necesidad que actualmente mantiene Chile en temas de delitos informáticos para mantener estos actos ilícitos regulados?

En conjunto con lo anterior, se busca responder a las siguientes preguntas: ¿Cuál será la mejor alternativa para Chile para regular las conductas ilícitas cometidas por medio de las tecnologías de la información y telecomunicaciones, las cuales afectan al comportamiento de la sociedad? Mediante la implementación de un marco legal actualizado en términos de delitos informáticos ¿Será necesaria la implementación de recursos u otros medios, tales como campañas publicitarias, nuevas políticas que ayuden con la sensibilización de la sociedad sobre el cuidado de sus datos personales? Un aspecto muy importante, como se planteó en la problemática, es la inexistencia de una ley actualizada que sancione los delitos informáticos actuales, lo que podría afectar la integridad de los datos de los involucrados.

## SOLUCIÓN PROPUESTA

### Características de la solución

El presente estudio analizó el estado del arte actual dentro de los ministerios chilenos y partes que conforman la comisión interministerial que supervisa el proyecto conducente a la adhesión del Convenio de Budapest en Chile. Esta investigación se llevó a cabo por medio de los recursos presentados en la Ley N° 20.285 Sobre Acceso a la Información Pública (Presidencia, 2008), con lo que se obtuvo la información relevante al tratado en Chile; también por medio de esta solicitud de información se solicitaron estadísticas de los ilícitos investigados y sancionados por la Ley N° 19.223 de delitos informáticos y la información relevante a proyectos de ley que fueron desarrollados por la Honorable Cámara de Diputados de Chile para realizar la modificación de la actual ley vigente de delitos informáticos.

Otro punto importante, fue el desarrollo de un estudio comparativo de la situación actual de los delitos informáticos. Este estudio se llevó a cabo mediante la comparación del análisis de los delitos tipificados en la legislación vigente chilena en materia de delitos informáticos contra la ley vigente de la República Dominicana, país que se encuentra adherido al Convenio de Budapest sobre la Ciberdelincuencia, quienes suscribieron en su totalidad los artículos descritos en el tratado (Europe, 2001). Mediante los resultados obtenidos se establecerá la brecha existente en la legislación actual chilena y la utilizada internacionalmente.

Otro punto importante de este estudio, es la realización de un análisis de jurisprudencias aplicadas en casos reales sancionados por la Ley N° 19.223 de delitos informáticos de Chile (Nacional, 1993). Este análisis consistió en desarrollar los casos seleccionados utilizando los artículos descritos en el Convenio de Budapest. Los resultados obtenidos describieron otro enfoque de sanción a los ilícitos descritos en los casos, lo que generó nuevas condenas y nuevas figuras penales por los cuales han sido desarrollados los juicios.

Por último, dentro del estudio desarrollado, es la presentación de un análisis, a las modificaciones a la actual Ley N° 19.223 de delitos informáticos chilena contrastada con el Convenio de Budapest. Con lo antepuesto, se identificaron las ventajas y desventajas, con las que contará Chile al realizar una de las opciones descritas anteriormente. Junto con lo anterior, proponer el desarrollo de un manual o la realización de talleres, capacitaciones que ayuden a llevar a cabo la unificación de criterios entre jueces y fiscales, para que los ilícitos que sean sancionados bajo una nueva legislación, ya sea con la adhesión al Convenio de Budapest o la modificación de la actual ley de delitos informáticos chilena, lo que deberá ayudar a la toma de decisiones para sancionar las conductas atípicas que son realizadas por medio de las tecnologías de la información.

### Propósito de la solución

El propósito de la solución es de identificar las diferencias de llevar a cabo la adhesión al Convenio de Budapest y la de actualizar la Ley N° 19.223 de delitos informáticos. Mediante el establecimiento de las diferencias entre ambas soluciones, se podrá conocer cuál o cuáles son las tipificaciones necesarias para tener una ley actualizada que sea adecuada para Chile y para los tiempos modernos. Junto con lo anterior, se establecerán las ventajas y desventajas de ambos modelos de soluciones propuestos en el estudio realizado.

De acuerdo a lo expresado anteriormente, se dieron a conocer las opciones que tiene Chile en temas de delitos informáticos. Entregar recomendaciones y observaciones sobre una modificación a la Ley N° 19.223 y la adhesión al Convenio de Budapest, reconociendo las ventajas y desventajas de cada situación, para que el poder legislativo pueda tener una visión más clara sobre las necesidades de Chile y establecer el camino más idóneo para el control sobre los delitos cometidos por medio de las tecnologías de la información.

Otro punto importante del estudio, será el de entregar una serie de recomendaciones. Dentro de estas recomendaciones se propondrán los lineamientos para realizar una política de concientización para los usuarios de las organizaciones, las que incluirán charlas introductorias a la seguridad de la información personal, sobre el uso seguro del internet, entre otras.

## OBJETIVOS Y ALCANCES DEL PROYECTO

### Objetivo general

Evaluar las ventajas y desventajas que tendrá la adherencia al Convenio de Budapest y un mejoramiento a la actual ley chilena de delitos informáticos, considerando los delitos que atenten contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos descritos en el tratado.

### Objetivos específicos

Dentro de los objetivos específicos es posible señalar los siguientes:

1. Determinar el estado del arte, marco teórico y casos de estudio de referencias para obtener una base de comparación.
2. Establecer la brecha entre la legislación chilena y el Convenio de Budapest sobre la Ciberdelincuencia.
3. Identificar y comparar las ventajas y desventajas de la adherencia al Convenio de Budapest y en la actualización a la Ley N° 19.223.
4. Evaluar casos de estudio real cometidos en Chile, aplicando los artículos del Convenio de Budapest sobre la Ciberdelincuencia.
5. Generar recomendaciones sobre la generación de políticas públicas de concientización social sobre el cuidado de la información personal.

### Alcances

Los alcances para el presente estudio son:

1. Se analizará la legislación chilena en materia de delitos informáticos (Nacional, 1993).
2. Se analizará la legislación chilena que se encuentre considerada dentro del Convenio de Budapest sobre la Ciberdelincuencia (Europe, 2001).
3. Se analizará la ley de delitos informáticos de un país que se encuentre adherido al Convenio de Budapest.
4. Se analizará la información obtenida mediante la utilización del recurso presentado por la Ley de Transparencia Sobre Acceso a la Información Pública (Presidencia, 2008), en donde se ha solicitado la información relevante para la realización del presente estudio.
5. Se analizarán casos reales acontecidos en Chile, donde se haya sancionado por la actual legislación chilena de delitos informáticos que involucren la interceptación y el acceso ilícito a información confidencial, delitos que atentan contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos u otros incidentes de seguridad.

### Limitaciones

En el desarrollo del estudio comparativo se presentaron las siguientes limitaciones:

* Falta de instrumentos de información, lo que imposibilitó conocer con exactitud el comportamiento de las consultas y estadísticas sobre delitos en un período determinado.

## METODOLOGÍAS Y HERRAMIENTAS UTILIZADAS

### Metodología a usar

El tipo de investigación emprendida se caracteriza por ser cualitativa descriptiva y bibliográfica (Kunz, 2005). El método empleado es el de inducción analítica, utilizando además para el desarrollo de esta tesis, el propio de la dogmática jurídica, y el método comparativo.

La técnica de investigación ha sido la generación de hipótesis, desde la perspectiva *lege ferenda*  (Rodríguez, 2008), pretendiendo a través de un análisis crítico a la legislación vigente sobre delitos informáticos, analizar la pertinencia de incorporar nuevas normas penales al ordenamiento nacional. Asimismo se realizó el análisis de la legislación extranjera, y se consultaron y compararon distintos ordenamientos jurídicos en lo que respecta a los delitos informáticos, especialmente de República Dominicana, y el Convenio de Budapest sobre la Ciberdelincuencia.

Para la obtención de datos se relevaron especialmente, fuentes documentales o secundarias, analizando sentencias, así como artículos e informes elegidos a partir de una investigación del material disponible y válido por sus contenidos para ser aplicados en la temática de este estudio. También se utilizaron estadísticas relacionadas con la presente investigación, realizadas por distintos organismos públicos de Chile. Descrito lo anterior, se tendrá considerado la realización de las siguientes fases para desarrollar el presente estudio:

1. Selección de un país que se encuentre adherido al Convenio de Budapest sobre la Ciberdelincuencia.
2. Estudio de la legislación chilena en temas de delitos informáticos y la del país seleccionado para realizar el análisis de derecho comparado.
3. Estudio de información pública obtenida por ley de transparencia sobre la materia estudiada.
4. Desarrollo de un estudio comparativo entre legislación chilena de delitos informáticos y la del país seleccionado.
5. Entrevista personal con experto en la materia
6. Análisis de casos de estudio de ilícitos sancionados por la Ley de Delitos Informáticos chilena cometidos en Chile.
7. Realizar un análisis del sector legislativo chileno en términos de delitos informáticos y al país seleccionado para el presente estudio.
8. Establecer las ventajas y desventajas de realizar la adhesión al Convenio de Budapest y de la actualización de la ley vigente de delitos informáticos.

### Herramientas de desarrollo

Se utilizarán leyes internacionales y nacionales, documentación pública y privada de Chile relacionada con los delitos informáticos:

* Convenio de Budapest sobre la Ciberdelincuencia (Europe, 2001).
* Decreto exento N° 3265, Crea comisión de trabajo interministerial conducente a la adhesión de Chile a la convención sobre ciberdelitos del consejo de Europa (Interior, 2009).
* Revista chilena de derecho y tecnología, La Convención sobre Cibercrimen del Consejo de Europa (Derecho, 2012).
* Ley N° 19.223 de Delitos Informáticos de Chile (Nacional, 1993).
* Información obtenida por ley de transparencia de información pública.

## ORGANIZACIÓN DEL DOCUMENTO

La presente tesis se encuentra estructurada mediante el desarrollo de cinco capítulos. Los contenidos del estudio se ordenan de una forma estructurada para obtener una mejor una mayor comprensión de los temas tratados, lo que es presentado de la siguiente forma:

1. El segundo capítulo del presente estudio, presenta la información sobre los elementos que fueron utilizados para la presente investigación:
2. Ciberdelincuencia
3. Convenio de Budapest sobre la ciberdelincuencia
4. Ciberdelitos en Chile
5. Decreto N° 3265, crea comité interministerial sobre ciberseguridad
6. Proyectos de modificación Ley N° 19.223 de delitos informáticos
7. Postura de Chile ante el Convenio de Budapest

1. Seguido de lo anterior, en el tercer capítulo se constituye por un estudio comparativo de legislaciones de países Latinoamericanos. La comparación se basó en las normativas vigentes que tengan contemplados los delitos informáticos en sus cuerpos. Las legislaciones comparadas corresponden a Argentina, Brasil, Chile, Colombia, Perú, Puerto Rico, República Dominicana, Uruguay, Venezuela.
2. En el cuarto capítulo, se recapituló información contenida en la legislación chilena. La obtención de la información se desarrolló por medio de la consulta a través de la Ley de Transparencia, en donde se obtuvo información relevante tanto para estadísticas de delitos informáticos y sobre la adherencia al Convenio de Budapest sobre la Ciberdelincuencia de Chile.
3. Para dar término al presente estudio, en el capítulo quinto, se lleva a cabo la evaluación y análisis de los resultados obtenidos en los capítulos anteriores. Estos resultados se han enfocado en la comparación de legislaciones internacionales, estudio de casos reales que han sido sometidos a juicio bajo la Ley 19.223 y estos mismos se desarrollaron bajo el Convenio de Budapest. Junto con lo anterior, también se entregó información relevante a los delitos de sabotaje y espionaje informático que han sido investigados y sancionados a lo largo del país.
4. Para finalizar este trabajo se exponen los resultados de la investigación en el capítulo de conclusiones del estudio. En este apartado se concluyen los resultados positivos y negativos, indicando los trabajos futuros que puedan quedar inconclusos o posibles desarrollos.

# REVISIÓN CRÍTICA DEL ESTADO DEL ARTE

En este capítulo se exponen los conceptos teóricos relevantes del presente trabajo de tesis. Primero se analizará el concepto de ciberdelincuencia, detallando los tipos de ilícitos que actualmente se encuentran vigentes según las Naciones Unidas (*UN*). Luego se realizará una definición del Convenio de Budapest sobre la Ciberdelincuencia. Para seguir con los temas relevantes al estudio presentado, se presentará el significado de la ciberdelincuencia en Chile, seguido de la descripción de la Ley 19.223. Para seguir con las normativas chilenas, se desplegarán los proyectos de leyes que se han desarrollado para la actualización de la actual ley de delitos informáticos, siguiente con la explicación del Decreto N° 3265 que crea Comité Interministerial sobre Ciberseguridad.

### Ciberdelincuencia

Cibercrimen, piratería, delincuencia informática, son muchos de los términos utilizados para definir un concepto tan amplio como es el de la ciberdelincuencia. Con el fin de tener una idea en común, se puede definir la ciberdelincuencia como el “*conjunto de aquellas acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito*” (Mexía, 2009). En otras palabras, se trata de una categoría de crimen tradicional que utiliza las tecnologías de información y telecomunicación para desarrollarse.

Una de las razones porque el cibercrimen es tan diverso, es por la cantidad delitos que se pueden cometer. Los delitos que se pueden desarrollar por medio de las tecnologías de la información y telecomunicación se pueden vincular los actos criminales tradicionales, como robos, suplantación de identidad, fraude, acoso por nombrar algunos, los cuales, en este caso, sean cometidos a través de la red. De acuerdo a las Naciones Unidas (*UN*), en su *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, desarrollado en Viena (Austria) del 10 al 17 de abril de 2000, se describen ocho tipos de delitos informáticos (Unidas, 2000):

* Espionaje industrial

Los delincuentes que utilizan las tecnologías de información, pueden realizar tareas de espionaje para las empresas que contratan sus servicios o bien para su beneficio propio. El espionaje tiene por finalidad obtener información confidencial, secretos comerciales o estrategias de comercialización. (Unidas, 2000).

* Sabotaje de sistemas

Usuarios con fines maliciosos atacan los sistemas de información de una determinada organización con el fin de impedir que los usuarios que requieren de este puedan acceder al sistema que ha sido atacado. Un tipo de ataque consiste en el envío de “*mensajes*” repetidos a una dirección o a un sitio electrónico, impidiendo así que los usuarios tengan acceso al sistema. (Unidas, 2000).

* Sabotaje y vandalismo de datos.

Consiste en obtener acceso a sitios electrónicos o bases de datos y borrar o cambiar los datos contenidos en estos. Mediante esta acción se corrompen los datos mismos y causando perjuicios. (Unidas, 2000).

* *Phishing*

Radica en el engaño a los usuarios para que revelen sus datos personales interponiendo sitios web falsos, los que son similares a los que son accedidos por estos. Esta información obtenida por los delincuentes puede ser usada para cometer ilícitos, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo. (Unidas, 2000).

* Pornografía infantil

La distribución de pornografía infantil a través del internet está en aumento. Esta problemática se agrava con la aparición de nuevas tecnologías, como por ejemplo la criptografía, la que es utilizada para esconder pornografía infantil que se transmita o archive. (Unidas, 2000).

* Juegos de azar

Los juegos azar electrónicos han tenido un incremento a medida que el comercio brinda facilidades de crédito y transferencia de fondos. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. (Unidas, 2000).

* Fraude en internet

Se denomina así, a un correo electrónico o página web fraudulenta, que pretende estafar económicamente por medio del engaño, generalmente presentado como donación a recibir, lotería o premio al que se accede previo envío de dinero. (Unidas, 2000).

* Blanqueo de dinero

Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones. (Unidas, 2000).

### Convenio de Budapest sobre la Ciberdelincuencia

El Convenio de Budapest sobre la Ciberdelincuencia, fue desarrollado por el Consejo de Europa. Este tratado fue firmado en Budapest el 23 de noviembre del 2001; su entrada en vigor fue el 1 de julio de 2004, teniendo como finalidad, proteger a la sociedad frente a la ciberdelincuencia, con la adopción de una legislación apropiada y de cooperación internacional entre los Estados miembros del consejo (Europe, 2001).

Según el *Observatorio Iberoamericano de Protección de Datos*, actualmente es el único acuerdo internacional que cubre todas las áreas importantes de la legislación sobre delitos informáticos (derecho penal, derecho procesal y cooperación internacional) (Oiprodat, 2014). Este tratado reconoce como necesidad legislar sobre el correcto desarrollo y utilización de las tecnologías de información. También dentro del desarrollo del tratado se establecen medidas que previenen actos maliciosos sobre los sistemas informáticos y de las tecnologías de la información, que puedan atentar contra la disponibilidad, confidencialidad e integridad de los datos que utilizan estas tecnologías. Estas medidas son tipificadas o descritas en el Convenio de Budapest, las que buscan evitar el abuso de sistemas, redes y datos, describiendo herramientas y métodos que otorgan facultades para la investigación y la sanción, tanto a nivel nacional como internacional, estableciendo medidas que permiten el mutuo acuerdo de cooperación entre los países adheridos al presente tratado.

Este tratado establece una legislación uniforme para los Estados miembros del Consejo de Europa (47 miembros y 8 observadores), descritos en el Anexo A. El convenio se encuentra abierto a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU, referidos en el Anexo B.

Según el Convenio de Budapest sobre la Ciberdelincuencia (Europe, 2001), propone como definición de delito informático como, “*los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos*”. En conformidad con lo dicho anteriormente, el tratado propone una clasificación de los delitos informáticos, la que está comprendida en cuatro grupos:

* Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

Antes de dar inicio con las definiciones de los tipos de delitos que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos, se debe entender que significan estos términos. La confidencialidad, es la propiedad de los datos, que busca que estos no sean revelados a personas que no cuentan con los permisos necesarios para acceder a ella (Guatemala, 2014); La integridad, es la propiedad que busca mantener los datos contenidos en un sistema de información libres de alteraciones no autorizadas (Guatemala, 2014); por último la disponibilidad, es una característica de la información, la que debe encontrarse a disposición de las personas autorizadas que la requieran (Guatemala, 2014). Teniendo estos puntos, se puede entender de mejor forma los conceptos relacionados con los tipos de delitos que se desarrollan a continuación.

* *Acceso ilícito a sistemas informáticos*. Se entiende por acceso ilícito a todo acto relacionados con la intrusión dolosa sin los permisos necesarios a un sistema de tratamiento de información (Luis de la Corte Ibáñez, 2014).
* *Interceptación ilícita de datos informáticos*. La interceptación ilícita se entiende por todo acto doloso que utilice las tecnologías de información para interceptar datos contenidos en un sistema informático, ya sea en una red pública o privada (Luis de la Corte Ibáñez, 2014).
* *Interferencia en el funcionamiento de un sistema informático*. La interferencia del funcionamiento de un sistema, se entiende como la obstaculización dolosa del funcionamiento de un sistema informático, mediante la utilización de tecnologías de información, provocando alteración, borrado, daños, de los datos contenidos en este (Luis de la Corte Ibáñez, 2014).
* *Abuso de dispositivos que faciliten la comisión de delitos*. El abuso de los dispositivos, se define como la acción que contempla la obtención de medios informáticos, como piezas de software o dispositivos informáticos, para obtener acceso ilícito a un sistema de información de forma total o parcial a los datos contenidos en este (Luis de la Corte Ibáñez, 2014).

Como se ha revisado en las definiciones de los delitos, estos atentan contra la confidencialidad, la integridad y la disponibilidad de los datos, lo que los expone a acciones delictivas. Existen muchas formas de cometer un ilícito que provoque la ruptura de estas definiciones, algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de *spyware* y de *keylogger*.

Siguiendo con la clasificación de los delitos descrita por el Convenio de Budapest, se encuentran los delitos informáticos. Estos actos se definen como una conducta diri­gida contra los datos contenidos en un sistema de información. Ahora bien, dentro de estas conductas, se pueden diferenciar dos tipos:

* *Falsificación informática*. La falsificación informática, se define como la acción que realizada mediante la introducción, alteración, borrado o supresión de datos informáticos, que originen datos no fidedignos, con la finalidad que sean utilizados como datos auténticos (Luis de la Corte Ibáñez, 2014).
* *Fraude informático*. El fraude informático es la conducta ilícita que causa perjuicios monetarios al usuario, mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos (Luis de la Corte Ibáñez, 2014).

Observando las definiciones de los ilícitos anteriormente detallados, se puede deducir que son todos aquellos que atentan con los datos de un sistema de información. Mediante esta definición, se puede indicar como ejemplo una intrusión llevada a cabo en una base de datos de un banco, en donde se alteren la información de las cuentas de usuarios, para que ellos puedan obtener un beneficio propio por medio de la alteración de los datos contenidos en los sistemas.

Otro tipo de delito considerado por el tratado, son los relacionados con el contenido. En esta clasificación se encuentran los ilícitos que se encuentran vinculados con la pornografía infantil.

* *La pornografía infantil*. Todas las actividades que conlleven a la producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos (Luis de la Corte Ibáñez, 2014).

Por último, los delitos relacionados con infracciones a la propiedad intelectual y derechos afines. Este tipo de accionar involucra los ámbitos de obras literarias, música, cine o video por medio de sistemas informáticos. Este ilícito, es comúnmente llamado piratería y puede generar graves perjuicios económicos para los autores o firmas que tienen los derechos de reproducción de los obras que han sin copiadas de ilícita.

### Ciberdelitos en Chile

El constante avance tecnológico que experimenta la sociedad, supone una evolución en las formas de cometer delitos, como también a la aparición de nuevos actos ilícitos. El delito informático se entiende como toda acción atípica, dolosa, cometida contra las personas, mediante la utilización de sistemas de tratamiento de información, con la intención de generar perjuicios que dañen la integridad, confidencialidad y disponibilidad de la información del usuario que haya sido víctima de estas acciones (Huerta & Libano, 1998).

Los ciberdelitos en Chile son un acto que se encuentra penado por la Ley 19.223 de delitos informáticos. La normativa actual de la materia en estudio, se encuentra configurada por cuatro artículos, los que a su vez tipifican los delitos de sabotaje y espionaje informático. Ahora bien, de acuerdo a los tiempos modernos han surgido figuras que contemplan el uso de las tecnologías de la información para desarrollar actos ilícitos que no se contemplan en la ley nacional como el *phishing* y el *hacking* y a su misma vez, los delitos son cada vez más difíciles de poder perseguir, por la razón que los infractores se encuentran radicados en otros países y la normativa nacional, no tiene las facultades necesarias para dar con los delincuentes informáticos.

### Decreto N° 3265, crea comité interministerial sobre ciberseguridad

El Decreto N° 3265 (Interior, 2009), dictamina la creación del Comité Interministerial sobre Ciberseguridad en Chile. Este tiene por finalidad asesorar a la Presidencia de la República en temas relacionados con la adhesión al Convenio de Budapest sobre la Ciberdelincuencia. Cuando fue dictaminado el presente comité, se determinó que deberá estar integrado por las siguientes partes, las cuales deberán ser partícipes de las decisiones tomadas por la Presidencia de la República en temas relacionados con la adhesión al tratado:

* Un representante de la Dirección de Seguridad Internacional y Humana del Ministerio de Relaciones Exteriores.
* Un representante del Ministerio Secretaría General de la Presidencia.
* Un representante de la Subsecretaría de Telecomunicaciones del Ministerio de Transportes y Telecomunicaciones.
* Un representante del Ministerio de Justicia.
* Un representante de la Agencia Nacional de Inteligencia.
* Un representante de la Policía de Investigaciones de Chile.
* Un representante de Carabineros de Chile.
* Un representante del Ministerio Público.
* Un representante de la División de Informática del Ministerio del Interior.
* Un representante de la División Jurídica del Ministerio del Interior.
* Un representante del Ministro del Interior, quien será su Secretario Ejecutivo.
* Un representante de la Subsecretaría del Interior.

Este comité podrá invitar a participar a funcionarios de la Administración del Estado u otras autoridades públicas, así como a representantes de entidades internacionales, públicas o privadas, académicas y de agrupaciones de la sociedad civil o del sector privado.

### Proyectos de modificación ley N° 19.223 de delitos informáticos

Desde la promulgación en el año 1993 de la ley de delitos informáticos chilena, hace más de veintitrés años atrás, no ha sufrido cambios en su cuerpo legal. Después de nueve años desde su entrada en vigencia, en el 2002, se realizó la primera solicitud de modificar y adecuar esta normativa de acuerdo a los cambios desarrollados por el avance de las tecnologías de la información y comunicación, en adelante *TIC*.

Recapitulando lo dicho anteriormente, al momento de la presentación y promulgación de la Ley 19.223 de delitos informáticos chilena, el acceso a internet era inexistente de forma masificada, como lo es en la actualidad. Este acceso ha ido en evolución con el pasar de los años. Durante el año 2016, según en la encuesta realizada por la Subsecretaría de Telecomunicaciones, se indicó que durante el año 2015, en Chile la penetración de internet en los hogares chilenos alcanzó un 71.6% (telecomunicaciones, 2016), lo que genera que existe un alto índice de la población que tiene acceso a las redes digitales y significando que los datos, tienen una mayor exposición en internet.

Por otra parte, la evolución de las TIC, ha generado que las conductas ilícitas, que utilizan medios informáticos progresen en su forma de cometido. Estas conductas han convertido en una necesidad la revisión completa de la estructura y contenido de la actual ley de delitos informáticos, con la finalidad ineludible de realizar una actualización, que sea acorde a esta nueva realidad o bien considerar la adhesión a un tratado internacional que tenga tipificadas estas conductas en su cuerpo legal.

Dicho lo anterior, en la Honorable Cámara de Diputados de Chile se han desarrollado cuatro proyectos de modificación a la actual ley de delitos informáticos (Chile C. d., 2002). Las modificaciones a la Ley 19.223, no han sido llevadas a cabo, siendo archivadas o se encuentran en tramitación en el Congreso Nacional, estas se describen en la tabla 2.1.

Tabla 2.1 Proyectos de modificación Ley 19.223. Fuente: Elaboración propia (2016)

|  |  |  |  |
| --- | --- | --- | --- |
| Ingreso | Título | Estado de Tramitación | N° Boletín |
| 19 de Junio de 2002 | Modifica la ley Nº 19.223, de 1993, que tipifica figuras penales relativas a la informática. | Archivado | 2974-19 |
| 03 de Agosto de 2010 | Modifica ley N° 19.223, con objeto de establecer sanciones para los funcionarios públicos que, sustraigan datos contenidos en los sistemas de información de sus respectivos servicios. | En tramitación | 7090-07 |
| 15 de Abril de 2015 | Modifica la ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática, sancionando la distribución, exhibición o reproducción de material pornográfico infantil. | En tramitación | 9998-07 |
| 18 de Junio de 2015 | Tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223. | En tramitación | 10145-07 |

De acuerdo a los datos expuestos en la Tabla 2.1, se observan cuatro proyectos que tuvieron como ambición modificar la Ley N° 19.223 de delitos informáticos nacional. De acuerdo a los proyectos desarrollados y entregados a la Honorable Cámara de Diputados de Chile, se llevaron a cabo los siguientes proyectos 2979-19, 7090-07, 9998-07 y el 10145-07.

El primer proyecto de ley 2974-19, ver Anexo K, desarrollado en el año 2002, fue derogado y archivo mientras no fuera modificado el artículo 18 del código penal chileno. Este proyecto indagaba en las protecciones legales ante acciones ilícitas que buscaban robar, destruir o negar el acceso a información sensible y valiosa, es decir, el acceso no autorizado a sistemas de datos, procesamiento o comunicación electrónica (Chile C. d., 2002), mediante la sustitución de los tres primeros artículos.

En segundo lugar, se encuentra el proyecto de ley 7090-07, descrito en el Anexo L, desarrollado en el año 2010. Esta intención de modificación a la normativa, se encuentra en tramitación, es decir, que aún se encuentra en la Cámara de Diputados del Congreso de Chile, en conversaciones entre los diputados presentes. El objetivo de modificación era de generar un quinto artículo en la Ley 19.223, que buscaba sancionar a los funcionarios públicos antes de ser desvinculados por actos que atenten contra la integridad y disponibilidad de un sistemas de tratamiento de información (Chile C. d., 2002).

El proyecto 9998-07, descrito en el Anexo M, al igual que el anterior, se encuentra en tramitación en la Cámara de Diputados de Chile. Este buscaba insertar un quinto artículo en la de delitos informáticos, con el que se quería calificar como delito informático la producción, venta, distribución, exhibición, por cualquier medio web de material pornográfico infantil, en cuya elaboración hayan sido utilizados menores de edad, aunque el material tuviere su origen en el extranjero o fuese desconocido, y la facilitación de dichas conductas información (Chile C. d., 2002).

Por último el proyecto de ley 10145-07, descrito en el Anexo N, encontrándose también en estado de tramitación. Este describe la solicitud de modificación de la Ley 19.223, proyecto que busca actualizar la actual norma de delitos informáticos. Uno de los tópicos para el proyecto, es la antigüedad de la presente ley, la que fue promulgada durante el año 1993. Junto con lo anterior, es evidente que la evolución de las *TIC*, así como de las actividades humanas vinculadas a ellas y las conductas ilícitas que se han desarrollado desde la promulgación de esta ley, es necesario una revisión a su estructura y contenido con la finalidad de actualizarla a esta nueva realidad.

De acuerdo a lo expuesto anteriormente, existen conductas, que difícilmente podrán sancionadas. Una de ellas, fue la defraudación que atentó contra el sistema de transporte público denominado Transantiago. Esta acción fue llevada a cabo por medio de un aplicativo que permitía llevar realizar una estafa financiera dirigida al sistema (Mercurio, 2014). Otro ejemplo claro del desfase de nuestra legislación, en relación con la normativa procesal, es el hecho de que se encargue a las divisiones encargadas de la investigación de delitos informáticos de ambas policías (Carabineros de Chile y Policía de Investigaciones), la búsqueda de los computadores que han sido objeto de hurto o robo, por delitos con naturaleza informática sobre la que recae la especialización de estos recursos policiales (Chile C. d., 2002).

A pesar de los proyectos de ley que han sido revisados en la Honorable Cámara de Diputados, la ley de delitos informáticos sigue sin ser modificada. El sistema de revisión de los proyectos de ley ha sido deficiente. Cada sesión llevaba a cabo en el Congreso Nacional, en donde se someten a votación los proyectos de ley con las “mejoras” a la presente ley de delitos informáticos, no se ha dado la importancia a la dado la voz a personas que sean especialistas en la materia, es decir, se centra en personas que han resuelto archivar o dejar en tramitación proyectos de ley, sin tener un conocimiento previo de lo que significa un delito informático. Sin embargo, hay delitos que se encuentran vinculados con la utilización de las TIC, como la pornografía infantil y los delitos relacionados con la propiedad intelectual, actos que cuentan con normativas actualizadas que cubren gran parte del espectro del delito.

### Postura de Chile ante el Convenio de Budapest

Chile es un país líder en penetración de celulares en la región y con uno de los índices de [acceso a banda ancha](http://www.latercera.com/noticia/negocios/2014/05/655-578040-9-chile-es-el-pais-con-mayor-penetracion-de-banda-ancha-en-america-latina.shtml) (telecomunicaciones, 2016). Sin embargo, la tecnología, no marcha a la par de la legislación digital nacional. La legislación actual sobre delitos informáticos, fue creada cuando internet en nuestro país era una realidad para una minoría. La presente ley esambigua y poco clara en sus definiciones y en su categorización de delitos. De ahí que diferentes organizaciones y expertos solicitan una actualización, la que hasta la fecha no ha sido pronunciada.

En Chile, el proyecto con el cual se formulaba formalmente la adherencia al Convenio de Budapest desarrollado por los diputados Marcela Sabat y Víctor Torres, el que contó con 44 votos a favor, no fue aprobado por la Cámara de Diputados (Chile C. d., 2011). De acuerdo a la Diputada Marcela Sabat, “*hace algunos años se decidió constituir una mesa de trabajo interministerial, esta era tan ambiciosa que finalmente quedó en nada*”. Esta mesa de trabajo interministerial, tenía como finalidad, asesorar a la Presidencia de la República en temas relacionados con la adhesión al Convenio de Budapest sobre la Ciberdelincuencia.

Hasta ahora, fuera del Viejo Continente, lo han suscrito Canadá, Japón, África del Sur y Estados Unidos. Durante el año 2007 se le extendió la invitación a Chile a formar parte del tratado, razón por la cual durante el año 2009, se creó la Comisión de Trabajo Interministerial sobre Ciberseguridad (Interior, 2009), con el objetivo de coordinar los requerimientos y acciones conducentes a la adhesión de Chile a la Convención. Luego en Agosto de 2014, el Ministro del Interior y Seguridad Pública manifestó el compromiso de realizar una política pública sobre Ciberseguridad, lo cual reactivó la Comisión con la finalidad de concluir la adhesión al convenio.

Durante una entrevista sostenida al diario La Estrategia, según Eduardo Vergara, Jefe de la División de Seguridad Pública de la Subsecretaría del Interior del Gobierno de Chile (Estrategia, 2016), la adhesión al Convenio Europeo de Ciberdelincuencia, implicaría grandes cambios en la actual legislación vigente. Estos cambios impondrían la necesidad de actualizar la ley 19.223, tipificando sobre nuevos delitos informáticos, como el *phishing*, estableciendo responsabilidades penales y también modificaciones organizativas, ya que el Convenio de Budapest conlleva la creación de organismos internos capacitados para desarrollar labores relacionadas con la transmisión instantánea de información y el establecimiento de un punto de contacto 24 horas al día, durante los 7 días de la semana.

Durante la formulación del proceso de adhesión, el Gobierno de Chile, ha decidido realizar la reserva de cinco artículos, los cuales no se adecuan a la legislación nacional. De acuerdo a las definiciones desarrolladas en el Convenio de Budapest los artículos 4, 6, 22 y 29, Ver Anexo H, tienen directa relación con la tipificación de actos deliberados e ilegítimos, los que también hablan de la venta y distribución de material fraudulento, mientras que el artículo N° 9 que habla sobre delitos relacionados con la pornografía infantil, se encuentra contenido en la Ley N° 20.526 (Justicia, 2011) que sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil.

# ESTUDIO COMPARATIVO

En este capítulo se desarrolló un estudio comparativo de países que cuentan con normativas dedicadas a sancionar los delitos informáticos. Para realizar la comparación, se consultaron las legislaciones de países latinoamericanos, que enmarcaran los delitos informáticos. Junto con lo anterior, se confeccionó un cuadro comparativo donde se expusieron los ilícitos que utilizan las tecnologías de información descritos en el Convenio de Budapest sobre la ciberdelincuencia (Europe, 2001), para identificar y tener una mayor claridad de la normativa utilizada para sancionar los actos delictivos por los países estudiados.

## ESTUDIO COMPARATIVO

El estudio comparativo, es la disciplina que estudia a los diversos sistemas jurídicos existentes para descubrir sus semejanzas y diferencias (García, 2004). Dicho esto, se analizarán las normas jurídicas en temas de delitos informáticos de los países de Argentina, Brasil, Chile, Colombia, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela. Estos países han sido descritos en el “*Informe Sobre Amenazas a la Seguridad en Internet*” (Symantec, 2012), en donde fueron evaluados los países de la región de América, en temas de generación de actividad maliciosa (que incluye Norteamérica y Latinoamérica), siendo esta donde se origina la mayor cantidad de actividad maliciosa a nivel mundial.

### Argentina

A partir de Junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos”, ha incorporado y realizado una serie de modificaciones al código penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (en adelante *CP*) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del *CP* vigentes actualmente. Se modificó el epígrafe del capítulo III cuyo nuevo título es "*Violación de Secretos y de la Privacidad*". Junto con lo anterior, se incluyeron los artículos 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255 en los cuales se ha modificado el *CP*. También hubo está la derogación del artículo 78 y 117 (Argentino, 2008).

Con esta actualización a la ley de delitos informáticos argentina, se pudo establecer nuevas tipificaciones no contempladas en el *CP*. Las actualizaciones realizadas han dado origen a una serie de penas que deberán ser cumplidas en caso de realizar alguna infracción al *CP*. También estos nuevos artículos han dado origen a definiciones de actos maliciosos que no se encontraban tipificados en la antigua ley.

### Brasil

La Ley N° 12.737 relativa a los delitos informáticos, promulgada en el año 2012, tipifica los delitos informáticos y junto con ello, modifica el código penal (en adelante CP). Dentro la ley, se incorporan en su cuerpo los artículos 154-A y 154-B. El primero de ellos, el artículo 154-A, describe los actos que serán sancionados mediante la intervención de un dispositivo ajeno, conectado o no a la red de ordenadores, vulnerando los mecanismos de seguridad con el fin de obtener, adulterar o destruir datos o información sin la autorización del titular del dispositivo o instalar vulnerabilidades para obtener ventaja ilícita, estableciendo las condenas de acuerdo a los actos descritos anteriormente. Mientras tanto, el segundo artículo, el 154-B, describe penas en caso que los actos definidos en el primer artículo atenten contra el servicio público y la seguridad del país.

De acuerdo a lo anterior, la Ley N° 12.737 también incluye una modificación a los artículos 266 y 298 del CP. El artículo 266, tipifica la interrupción del servicio de telecomunicaciones, mientras que el artículo 298, habla sobre la falsificación de tarjetas. Por otra parte, la Ley 11.829, promulgada durante el año 2008 regula el combate y prevención de la pornografía infantil por medios de sistemas informáticos (Brasileña, 2012).

### Chile

La Ley 19.223 relativa a delitos informáticos, promulgada en el año 1993. Esta normativa desde el año de su promulgación no sufrido modificaciones en su cuerpo legal. Lo que no se puede dejar de mencionar, ha sido los intentos que se ha tenido por realizar modificaciones por parte de la Honorable Cámara de Diputados en el Congreso de Chile. Desde la fecha se han realizado 4 proyectos de modificación. Esta normativa, está conformada por cuatro artículos, desde los cuáles se tipifican dos delitos informáticos, espionaje y sabotaje informático.

La Ley 17.336 relativa a los delitos que atentan contra la propiedad intelectual y derechos de autor. Esta normativa fue promulgada durante el año 1970, siendo una de las más antiguas puestas a disposición del presente estudio. Esta ley protege los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de obras de la inteligencia en los dominios literarios, artísticos y científicos, cualquiera que sea su forma de expresión, y los derechos conexos que ella determina. Así mismo el derecho de autor comprende los derechos patrimonial y moral, que protegen el aprovechamiento, la paternidad y la integridad de la obra (Chile C. n., 1970).

Por último cabe mencionar, la Ley 20.526 que sanciona el acoso sexual a menores, la pornografía infantil virtual y la posesión de material pornográfico infantil. Esta norma promulgada durante el año 2011, propone cambios en el Código Penal (en adelante CP) modificando el artículo 366 quáter, de la misma forma también se modifica la Ley 20.084 sustituyendo el artículo 4 y por último se solicita la sustitución en el Código Procesal Penal en su artículo 222 (Congreso, 2011).

### Colombia

La Ley 1.273, promulgada durante el año 2009, modifica el Código Penal. Esta disposición establece como un bien jurídico “la protección de la información y de los datos”. Dentro de esta nueva ley, se ha agregado el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", el cual contiene los artículos 269A, 269B, 269C, 269D, 269E, 269F, 269G, 269H que regulan una serie del figuras penales que atenten contra la seguridad de la información. Adicionalmente también se encuentra el CAPÍTULO II, nombrado “De las atentados informáticos y otras infracciones”, que contiene los artículos 269I y 269J, que describen acciones delictivas asociadas al hurto y transferencia con medios informáticos. Junto con lo anterior, también se incorpora el artículo 58, que considera como agravante la realización de alguna de las conductas anteriormente descritas, si se realizan por medios informáticos, electrónicos o telemáticos” (Comunicaciones, 2009).

Junto con la Ley 1.273, que modifica el CP, se encuentra la Ley 1.236 promulgada en el año 2008, por la cual se modifican los artículos del Código Penal relativos al abuso sexual. Dentro de esta ley, se encuentra el artículo N° 12, que modifica el artículo N° 218 de pornografía con menores, especificando las acciones que serán sancionadas por la legislación nacional (Colombia, 2008).

### Perú

La Ley 27.309 promulgada en el 2000, incorpora al Código Penal (en adelante CP) del Perú los Delitos Informáticos. Por medio de un artículo único que contiene los artículos 207-A, 207-B, 207-C y 208 que modifican el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo N° 635 (Peruana, 2000). Estos artículos ingresos dan origen a la tipificación de los actos relacionados con el acceso y utilización indebida, a los datos contenidos en bases de datos o sistemas de información. Junto con ello, se describen las penas que deberán ser ejecutadas cuando el individuo haga caso omiso a la presente ley.

Otra ley existente, la cual también ha sido modificada por el congreso peruano, es la Ley 28.251 promulgada en el 2004. Esta ley se actualizó mediante la modificación de los artículos 170, 171, 173, 174, 175, 176, 176-A, 179, 180, 181, 182, 183, 183-A y la incorporación de los artículo 179-A, 181-A, 182-A, a los capítulos IX, X y XI del título IV del libro segundo del *CP.* Los actos descritos en los artículos nombrados anteriormente, hacen relación a delitos que atentan contra la integridad sexual, no olvidando, la tipificación contra la pornografía infantil contenida en el artículo 183-A (Perú, 2004).

Por último, Perú posee la Ley 28.493 promulgada en el 2005 (Peruano, 2005), que regula el uso del correo electrónico no solicitado (*spam*). La presente ley, está compuesta por 11 artículos, en los cuales describe la regulación del envío de correos con fines comerciales o de otra índole, no solicitados por los usuarios. Esta ley, tiene una particular característica, la cual es no contar con sanciones de ningún tipo penal ante la infracción de la misma.

### Puerto Rico

A pesar que Puerto Rico, no presenta una ley específica que tipifique los delitos informáticos, se puede apreciar que existen leyes especiales y artículos del Código Penal (en adelante CP) que hacen referencia a este tipo de acciones. Dentro del CP, se encuentran los delitos:

* Contra la protección debida a menores, que comprende el artículo 124.
* De la obscenidad y la pornografía infantil, que comprende los artículos 144 al 152.
* Contra el derecho a la intimidad, que comprende los artículos 167 al 175.
* Contra la tranquilidad personal, que comprende los artículos 177 y 178.
* Contra los bienes y derechos patrimoniales, que comprende los artículos 181 al 188
* Relacionados con el fraude, que comprende los artículos 203 y 205.
* Relacionados con la usurpación de identidad, que comprende los artículos 208 y 209.
* Relacionados con las falsificaciones, que comprende los artículos, que comprende los artículos 211 al 213, 216, 217, 219, 228 y 229.
* Relacionados con la interferencia de los servicios públicos, que comprende el artículo 240.

Junto con lo dispuesto en el CP, se aprecia la existencia de las leyes especiales que tipifican ciertos actos ilícitos que utilizan las tecnologías para cometer infracciones. La Ley Núm. 43-1994 sobre ley especial penal de reproducciones, actuaciones en vivo y rotulación sin autorización del dueño, la Ley Núm. 165-2008, sobre la regulación de programación de espionaje cibernético (Cibernéticos, 2012).

### República Dominicana

Durante el año 2007, la República Dominicana, promulga la Ley 53-07 contra crímenes y delitos de alta tecnología. Ahora bien dicha ley, durante el año 2012, mediante la resolución N° 158-12 se aprueba la adhesión al Convenio sobre la ciberdelincuencia.

Ahora bien, durante el año 2013, República Dominica actualiza la Ley 53-07 sobre crímenes y delitos de alta tecnología. En esta actualización se desarrolla la adhesión al Convenio de Budapest sobre la ciberdelincuencia. Este acto, permitió alinearse con una legislación acorde a los tiempos modernos, capaz que poder controlar los actos ilícitos que utilizan las tecnologías de información (Dominicana, 2013).

### Uruguay

Uruguay ha resultado ser un país que no se ha evidenciado una legislación dedicada para la materia en estudio (delitos informáticos). Sin embargo, a pesar de no contar con una ley específica para los delitos informáticos, se han encontrado normativas que pueden ser aplicadas a la materia. La Ley N° 17.520, en su artículo N° 1, tipifica el uso indebido de señales destinadas para usuarios que se encuentran suscritos a ella (Uruguay, 2002). Por último la Ley Nº 17.815, promulgada durante el año 2004, regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contengan imágenes o cualquier otra forma de representación que sean violentados (oficial, 2004).

Como se habría mencionado Uruguay, no contempla una legislación especial para los delitos informáticos, por ende, cada acción delictiva se encuentra descrita indirectamente dentro de otras leyes. De acuerdo a lo anterior, los actos que atentan contra la integridad de datos y de la información, es posible poder sancionarlos mediante la Ley 18.600 de *Documento Electrónico y Firma Electrónica*. El artículo 4to, de la mencionada ley, se puede visualizar las acciones que serán sancionadas en caso de quebrantar la integridad de la información contenida en un documento electrónico (Legislativo, 2009).

Por último, cuando se habla sobre la integridad del sistema se evidencia dentro del CP los actos sancionados sobre sistemas de telecomunicaciones. Ahora bien, la legislación Uruguaya, contempla en el CAPÍTULO IV, el artículo 217, los ataques a los sistemas de telecomunicaciones (Uruguay I. -N., 1933).

### Venezuela

La ley especial contra delitos informáticos promulgada durante el año 2001 que tipifica los actos que atenten contra los sistemas o componentes de un sistema de información. Esta ley está compuesta por 33 artículos dispuestos en 5 Capítulos, que definen los delitos contra los sistemas que utilizan tecnologías de información; contra la propiedad; contra la privacidad de las personas y de las comunicaciones; contra niños, niñas o adolescentes y los delitos contra el orden económico (Venezuela, 2001).

### Tipificaciones de delitos informáticos según evaluación

Para analizar en profundidad los delitos contenidos en las leyes en materia de delitos informáticos de los países Argentina, Brasil, Chile, Colombia, Perú, Puerto Rico, República Dominicana, Uruguay y Venezuela se establecieron los actos ilícitos contenidos en el Convenio de Budapest (Europe, 2001). Los delitos contenidos en el tratado son, acceso ilícito, interceptación ilícita, ataques contra la integridad de los datos, ataques contra la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático y pornografía infantil.

En la Tabla 3.1, se aprecia cómo se encuentran identificados cada delito indicado anteriormente. Claramente, no todos los delitos contenidos en el Convenio de Budapest, se encuentran tipificados dentro de las legislaciones de los países analizados.

Tabla 3.1 Delitos contenidos en legislaciones de países analizados. Fuente: Elaboración propia (2016).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Actividad Maliciosa | Acceso ilícito | Interceptación ilícita | Ataques a la integridad de los datos | Ataques a la integridad del sistema | Abuso de los dispositivos | Falsificación informática | Fraude informático | Pornografía infantil |
| Argentina | Art. 153 | Art. 153 Bis | Art. 183 | Art. 183   Art. 197 | No hallado | Art. 292 | Art. 173 | Art. 128 |
| Brasil | Art. 154-A | No hallado | Art. 154-A | Art. 266 | Art. 154-A | No hallado | No hallado | Ley 11.829 |
| Chile | Art. 2 | Art. 2 | Art. 3 | Art. 1 | No hallado | No hallado | No hallado | Ley 20.526 |
| Colombia | Art. 269 A | Art. 269 C | Art. 269 D | Art. 269 B Y D | No hallado | No hallado | Art. 269 J | Art. 218 |
| Perú | Art. 207 A | Art. 207 A | Art. 207 B | Art. 207 B | No hallado | No hallado | No hallado | Ley 28.251  Art. 183 A |
| Puerto Rico | Art. 171 | Art. 171 | Art. 171   Art. 198 | Art. 186  Art. 240 | Art. 218 | Art. 213  Art. 217 | Art. 203 | Art. 146  Art. 147 |
| República Dominicana | Art. 2 | Art. 3 | Art. 4 | Art. 5 | Art. 6 | Art. 7 | Art. 8 | Art. 9 |

Tabla 3.1 Delitos contenidos en legislaciones de países analizados. Fuente: Elaboración propia (2016). (Continuación)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Actividad Maliciosa | Acceso ilícito | Interceptación ilícita | Ataques a la integridad de los datos | Ataques a la integridad del sistema | Abuso de los dispositivos | Falsificación informática | Fraude informático | Pornografía infantil |
| Uruguay | No hallado | Ley N° 17.520  Art. 1 | Ley N° 18.600  Art. 4 | Código Penal  Art. 217 | Ley N° 17.520  Art. 1 | No hallado | No hallado | Ley N° 17.815  Art. 2 |
| Venezuela | Art. 6 | Art. 21 | Art. 7 | Art. 7 | Art. 10  Art. 19 | Art. 12 | Art. 14 | Art. 24 |

Se observa la existencia de delitos que no se encuentran tipificados en las legislaciones de los países analizados. Dentro de la Tabla 3.1, se pueden apreciar delitos que no se encuentran considerados en las legislaciones de los países estudiados, como por ejemplo, el delito abuso de los dispositivos (Europe, 2001), fue posible encontrarlo tipificado en las legislaciones estudiadas, a excepción de la ley vigente en Brasil, Puerto Rico, República Dominicana, Uruguay y Venezuela.

Otro punto importante a destacar son las modificaciones a las leyes que contienen tipificados los delitos informáticos. En el estudio se apreció que hay normativas que se encuentran más actualizadas que otras, producto de las “*mejoras*” que han sido desarrolladas. En el caso de Chile, legislación que data del año 1993, se evidenció que es la más antigua dentro de las leyes analizadas, pero es la única que no sufrido modificaciones en su cuerpo, lo que ha generado que la tipificación de delitos sea acotada. En el caso de República Dominicana, se ha podido apreciar que este país se encuentra adherido al Convenio de Budapest. Visualizando la Tabla 3.1, se observa que la ley chilena, es capaz de tipificar dos actos ilícitos utilizando un mismo artículo, situación muy distinta a la apreciada con ley vigente de República Dominicana, que cada acto, se encuentra contemplado en artículos distintos.

De acuerdo a la situación descrita anteriormente, para el poder judicial chileno, esta situación puede generar confusión en el momento de tomar algún tipo de decisión al momento de establecer algún tipo de sanción. La confusión se puede originar, al estar dos tipos de delitos contenidos en un mismo artículo, lo que dejará directamente al criterio y conocimiento que el juez o el perito aplique sobre el acto en cuestión, situación que puede generar controversias en los fallos dictados por los jueces. Ahora bien, con la norma de la República Dominicana, la toma de una decisión por parte de un juez o un perito experto en la materia, no será de gran complejidad, ya que los delitos se encuentran tipificados adecuadamente en cada artículo de la ley vigente del mencionado país, lo que no deja al criterio de la autoridad la toma de una decisión.

## CONCLUSIONES

Para el desarrollo de este capítulo se desplegó un estudio comparativo de las legislaciones, en materia de delitos informáticos, de los países latinoamericanos abordados en el presente estudio. Se constató la existencia de países que no cuentan con una normativa exclusiva para este tipo de acto, como lo son Puerto Rico y Uruguay, mientras que otros si cuentan con una legislación dedicada para estos efectos, como por ejemplo República Dominicana, país que se encuentra adherido al Convenio de Budapest sobre la ciberdelincuencia. Junto con lo anterior, se construyó un cuadro resumen que permitió identificar los delitos informáticos, identificados en el Convenio de Budapest, que se encuentran tipificados en cada país abordado en el estudio y saber cuál es la norma o artículo con la que se atañe dicho ilícito.

# LEGISLACIÓN CHILENA

En este capítulo se exponen los temas relevantes sobre la propuesta de llevar a cabo la adhesión al Convenio de Budapest por parte del Gobierno chileno. Primero se expondrán las leyes vigentes de Chile, que se encuentran contenidas en los artículos del tratado. Seguido de lo anterior, se ha analizado la Constitución Política de Chile, en donde se ha hecho referencia al artículo 19 número cuatro, como una barrera constitucional que se verá enfrentado el proyecto de ley para la adherencia al Convenio de Budapest. Siguiendo con la legislación chilena, se realizado una investigación por medio de la Ley de Transparencia, para obtener estadísticas sobre los delitos informáticos cometidos en Chile. Por último, se analizaron juicios por infracción a la Ley 19.223, los que posteriormente fueron desarrollados bajo los artículos del Convenio de Budapest.

## LEGISLACIÓN CHILENA CONTENIDA EN CONVENIO DE BUDAPEST

Los avances tecnológicos y la masificación del acceso a internet, han abierto una brecha entre el accionar delictual de los usuarios mal intencionados y la legislación chilena de delitos informáticos. Sin embargo, a pesar de la brecha existente, hay delitos que han sido considerados en el transcurso del tiempo, modificándose a medida que han sufrido vacíos legales en sus líneas. Estos actos son los que tienen relevancia con la pornografía infantil y la propiedad intelectual e industrial. Cada uno de las acciones descritas anteriormente, cuentan con una legislación propia, descritas en la Tabla 4.1, que norma su accionar y sanciona su infracción.

Tabla 4.1 Leyes influenciadas por las tecnologías de la información. Fuente: Elaboración propia (2016)

|  |  |
| --- | --- |
| Ley N° | Nombre |
| Ley N° 20.526 | Sanciona el Acoso Sexual de Menores, la Pornografía Infantil Virtual y la Posesión de Material Pornográfico Infantil. |
| Ley N° 17.336 | Propiedad Intelectual y Derechos de Autor. |

Los actos descritos anteriormente, también son víctimas de las tecnologías de la información. Al encontrarse afectados por las tecnologías, sus normativas, deben considerar apartados especiales dentro de sus cuerpos que cubran la utilización de estas para llevar a cabo las infracciones.

Ahora bien, de acuerdo a lo descrito anteriormente, el Convenio de Budapest sobre la Ciberdelincuencia (Europe, 2001), cuenta con artículos destinados para estos fines. Los artículos en cuestión son 9° y 10°, descritos en el Anexo E. Estos artículos hacen mención a los delitos relacionados con la pornografía infantil y con infracciones a la propiedad intelectual y derechos afines, respectivamente.

## DERECHOS FUNDAMENTALES

El Convenio de Budapest sobre la Ciberdelincuencia tiene como espíritu la cooperación internacional. Dicha cooperación involucra compartir información sobre la utilización del internet por parte de los usuarios, es decir, compartir las acciones realizadas en la red desde las computadoras personales de los ciudadanos de los países que se encuentren adheridos al mencionado tratado.

De acuerdo a lo anterior, el tratado exige a los proveedores de internet (ISP, por sus siglas en ingles Internet Service Provider) que almacenen por un tiempo limitado de noventa días como máximo los datos de navegación. Se entiende como datos de navegación todos los datos vinculados a los sitios web que se visitan, como por ejemplo búsquedas llevadas a cabo en buscadores como Google, software que se descarguen (Europe, 2001).

De acuerdo a lo expresado anteriormente, Chile por su parte, se encuentra en una posición que los datos personales o los que afecten a la privada se encuentran protegidos constitucionalmente. La Constitución Política de Chile regula en el artículo 19 número cuatro(Chile C. P., 2005), que todos los ciudadanos chilenos cuenten con el respeto y protección de la vida privada y a la honra de la persona y su familia. Según la redacción del artículo, este hace mención en primer lugar al respeto a la vida privada, y la honra, resguardando dos derechos distintos. La honra, se entiende como la posición que ocupa una persona en las relaciones sociales (Egaña, 2003). Por otra parte, la vida privada se define como el conjunto de asuntos, conductas, documentos, comunicaciones, imágenes o recintos que, el ciudadano, no desea que sean conocidos por terceros sin su consentimiento previo (Egaña, 2003).

## LEY DE TRANSPARENCIA

La realización del presente estudio, se incluyeron estadísticas generadas a partir de una serie de datos obtenidos mediante mecanismos de recolección de información disponible. De acuerdo a la solicitud realizada por la Ley N° 20.285 (Presidencia, 2008), se elevó la solicitud de información relevante a delitos informáticos acontecidos durante el período 2010 al 2015 y sobre la adhesión al Convenio de Budapest por parte de Chile (ver Anexo I). Mediante la indagación, se ha recopilado información entregada por la Brigada de Investigación del Cibercrimen de la Policía de Investigaciones de Chile (ver Anexo J). Otras solicitudes de información, dirigidas al Ministerio del Interior y Seguridad Pública, Dirección General de Carabineros de Chile, Ministerio de Justicia y la Intendencia de la Región Metropolitana, no dieron lugar a respuestas con información de utilidad.

### Estadísticas de delitos informáticos

Las estadísticas de delitos informáticas en Chile, se ven reflejadas en la Tabla 4.2 corresponde al detalle de delitos que han sido investigados por la Policía de Investigaciones de Chile. Durante el período comprendido entre los años 2010 a 2015, que son 976.997 investigaciones, mientras que de este total se desprenden 3.500 investigaciones, que corresponden a delitos investigados por infringir la ley N° 19.223, correspondiendo un 0,36% del total de investigaciones.

*Tabla 4.2 Cantidad de delitos que han sido investigados por la Policía de Investigaciones de Chile. Fuente: Elaboración propia (2016)*

|  |  |  |
| --- | --- | --- |
| Año | Cantidad | Delitos informáticos |
| 2010 | 145.157 | 603 |
| 2011 | 160.927 | 795 |
| 2012 | 163.036 | 604 |
| 2013 | 165.062 | 456 |
| 2014 | 172.794 | 522 |
| 2015 | 170.021 | 520 |
| **Total** | **976.997** | **3.500** |

### Formalizaciones Delitos Informáticos

A partir de los datos entregados mediante la solicitud de información pública, se pueden interpretar las cifras anteriormente expuestas. Cabe señalar que todos estos datos abarcan el período comprendido entre los años 2010 a 2015.

De acuerdo a lo anterior, las investigaciones llevadas a cabo ascendieron a 976.997, durante el período mencionado anteriormente. Ahora bien, los procedimientos llevados a cabo bajo la Ley de Delitos Informáticos, fueron 3.500 ilícitos, lo que se describe en la Tabla 4.2, traduciendo esto en un 0,36 % del total de indagaciones durante el período comprendido para el presente estudio. Sin embargo, durante el período de estudio, existieron 28 detenidos por el delito de sabotaje informático y 22 por espionaje informático, del total de investigaciones llevadas a cabo por la Brigada de Ciberdelitos de la Policía de Investigaciones de Chile, lo que queda reflejado en la Tabla 4.3.

*Tabla 4.3 Detenidos por infracción a la Ley 19.223 por la Policía de Investigaciones de Chile. Fuente: Elaboración propia (2016)*

|  |  |  |
| --- | --- | --- |
| Año | Sabotaje informático | Espionaje informático |
| 2010 | 2 | 7 |
| 2011 | 3 | 0 |
| 2012 | 4 | 2 |
| 2013 | 7 | 2 |
| 2014 | 5 | 1 |
| 2015 | 7 | 10 |
| **Total** | **28** | **22** |

En el Figura 4.1, se presenta la evolución del número de detenidos por los delitos de espionaje informático, sabotaje informático del período 2010 - 2015. Es posible visualizar que en el período estudiado, la cantidad de imputados formalizados en términos totales ha aumentado de forma moderada pero constante. Por otro lado, el sabotaje y espionaje informático presentan un inicio ínfimo al inicio del período. Esto se puede explicar por el constante avance de las tecnologías de la información y de comunicaciones en los últimos años que ha tenido Chile.

Figura 4.1 Delitos informáticos período 2010 a 2015. Fuente: Elaboración propia (2016)

Durante el período comprendido entre los años 2010 - 2015, existieron 3.500 investigaciones llevadas a cabo por la Brigada de Ciberdelitos de la Policía de Investigaciones de Chile. De acuerdo a lo expresado en la Tabla 4.3, el delito que tuvo una mayor tasa de investigación fue el sabotaje informático, mientras que el de espionaje informático, muestra un leve crecimiento en comparación con su par. Durante los años 2012 y 2013, existió una tendencia a la disminución de investigación de ambos delitos, pero esto se ve mermado durante el año 2014 y 2015, que muestran un alza en la tasa de investigaciones llevadas a cabo, lo que se refleja en la Figura 4.2.

Figura 4.2 Delitos investigados por infracción a la Ley N° 19.223 periodo 2010 a 2015. Fuente: Elaboración propia (2016)

Ahora bien, en la Figura 4.3, se observa la relación de personas que han sido puestos a disposición de los tribunales por los delitos sabotaje y espionaje informático, que asciende a la cantidad de 50 imputados entre el período 2010 - 2015, lo que significa un 1.4% del total de delitos investigados por la Brigada de Delitos Informáticos, mientras que los delitos investigados ascendió a 3.500 dentro del mismo período.

Figura 4.3 Delitos puestos a disposición e investigados 2010 a 2015. Fuente: Elaboración propia (2016)

Otro punto importante a destacar, es lo observado en la Figura 4.4, la evolución de las personas que han sido puestas a disposición de los tribunales por infracción a la ley 19.223 de delitos informáticos, durante el período comprendido para el presente estudio. Bajo este contexto existió un total de 50 personas que fueron llevadas a tribunales por la Brigada de Ciberdelitos de la Policía de Investigaciones de Chile, las que quedado reflejadas en la Tabla 4.3. De acuerdo a lo expresado por los datos obtenidos, durante el año 2010, el delito que tuvo una mayor tasa de investigación fue el de espionaje informático, mientras tanto que el ilícito de sabotaje informático, disminuyó. Durante los años 2011 y 2012, la tasa de personas puestas a disposición de tribunales, por el delito de espionaje informático, tuvo una baja drástica, mientras que el de sabotaje se mantuvo en sus cifras.

Siguiendo con lo anterior, durante el año 2013 y 2014, el delito de sabotaje informático, mostro un crecimiento acelerado, en comparación con el año del inicio del estudio, mientras que el delito de espionaje, se mostró en bajada. Por último, durante el año 2015, el delito de espionaje informático, nuevamente se tornó en subida, siendo el delito que demostró tener más personas que fueron llevadas a tribunales, mientras que el de sabotaje, se mantuvieron, sin mostrar desviaciones.

Figura 4.4 Delitos puestos a disposición de tribunales por infracción a la Ley N° 19.223 periodo 2010 a 2015. Fuente: Elaboración propia (2016)

De acuerdo a las tipificaciones establecidas en la Ley 19.223 se establecen dos delitos el espionaje y sabotaje informático. Según los datos recogidos, se aprecia en la Figura 4.5 la cantidad de delitos relacionados con el espionaje informático, descrito en la legislación actual, se aprecia que durante el año 2014 en la Región Metropolitana, se produjo la mayor cantidad de delitos denunciados ante la Policía de Investigaciones de Chile, los que ascendieron a 69 acusaciones. Mientras que el año 2010 en la región de Magallanes y de la Antártica chilena, se aprecia que existieron 28 acusaciones por este ilícito.

Otro punto a destacar de la Figura 4.5, es la centralización de delitos de espionaje informáticos. El centro de delitos investigados radica en la región Metropolitana, donde se presentan las cantidad más altas de delitos investigados, seguido de esta, se destaca la región de Valparaíso. Ambas regiones no coinciden con los mismos índices de delitos investigados, pero sí, son las dos regiones que más actos ilícitos han sido denunciados e investigados.

Figura 4.5 Espionaje Informático a nivel nacional comprendido entre 2010 – 2015. Fuente: Elaboración propia (2016)

A continuación en la Figura 4.6 se visualiza la cantidad de delitos relacionados con el sabotaje informático a nivel nacional. En el gráfico se aprecia que durante el año 2010 en la Región Metropolitana, se produjo la mayor cantidad de delitos denunciados ante la Policía de Investigaciones de Chile, los que ascendieron a 433 acusaciones. Mientras que el año 2011 en la región de Antofagasta, se aprecia que existieron 136 acusaciones por este ilícito que fueron investigados.

Otro punto a destacar de la Figura 4.6, es la centralización de delitos de sabotaje informáticos. El centro de delitos investigados radica nuevamente en la región Metropolitana, donde se presentan las cantidad más altas de delitos investigados, seguido de esta, se destaca la región del Bío-Bío. Ambas regiones no coinciden con los mismos índices de delitos investigados, pero sí, son las dos regiones que más actos ilícitos han sido denunciados e investigados.

Es muy importante destacar que en las regiones de Tarapacá, Coquimbo, Magallanes y de la Antártica chilena y Arica y Parinacota, se han evidenciado los niveles más bajos a nivel nacional de delitos relacionados con el sabotaje informático. Para mayor detalle de los datos estudiados ver Anexo C.

Figura 4.6 Sabotaje Informático a nivel nacional comprendido entre 2010 – 2015. Fuente: Elaboración propia (2016)

## CASOS DE ESTUDIO

Uno de los puntos más importantes dentro del presente estudio, es la exposición de juicios cometidos en Chile, en los cuales se han formulado cargos por infracción a la Ley N° 19.223. De acuerdo a lo anterior, se han seleccionado los casos “*Hipermercado Curicó con Lizama Ponce, María de las Nieves y otros; Sky Chile CPA con Merino Moraga, Pablo Andrés; y Polincay Export y comercial Polincay limitada con Pérez Rodríguez”.* Junto con ello, se evidenciarán los cargos formulados para cada caso y las sentencias que han dictado los jueces que han sobrellevado la causa.

### Hipermercado Curicó Ltda. con Lizama Ponce, María de las Nieves

Los cargos presentados contra la cajera del hipermercado Curicó limitada, se basan en la Ley 19.223, artículo 1°. El primer artículo de la mencionada normativa, dice “e*l que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento”* (Nacional, 1993)*,* lo indicado en este artículo indica que toda mala utilización que fuese realizada con dolo, que provoque la disponibilidad de un sistema de información, podrá ser acusado de infringir la ley bajo el artículo mencionado.

De acuerdo a lo anterior, en este caso, la cajera es acusada de abusar de una falla del dispositivo. Esta vulnerabilidad en el aparato, corresponde a una falla en la programación realizada por el proveedor, situación que la cajera se percata y hace aprovechamiento de esta debilidad del aparato provocando un perjuicio económico al Hipermercado Curicó Limitada.

* Nombre del caso: “*Hipermercado Curicó Limitada con Lizama Ponce, María de las Nieves y otros*”.
* Cargos formulados*: “La Cajera de un supermercado se aprovecha del sistema de venta de tarjetas electrónicas de saldo para telefonía móvil para venderlas sin registrar la venta en el sistema interno de cajas*.

*Se formulan cargos, incluida la comisión del delito contenido en el artículo 1° de la Ley N° 19.223, en tanto se impide, obstaculiza o modifica el funcionamiento de un sistema de tratamiento de información*”. (Chile P. J., 2012).

Según lo descrito en los cargos sobre la cajera del supermercado, se declara que la acusada se aprovecha del funcionamiento erróneo del sistema para su beneficio propio. De acuerdo a lo anterior, los hechos implican que existió un aprovechamiento de una debilidad  
del sistema de las cajas del supermercado, si bien esta acción pudo haber sido realizada con dolo, es decir, que debieron tener la intención de ocasionar un daño monetario al dueño del supermercado. Ahora bien, de acuerdo al tribunal, la implicada en los hechos sólo se aprovechó de su funcionamiento, el cual se encontraba con defectos en su programación, acción que no se encuentra tipificada en la Ley N° 19.223 de delitos informáticos. Por lo tanto en este caso, no se pudo realizar una sentencia bajo la mencionada ley. Para mayor información del caso estudiado ver Anexo F.

### Sky Chile CPA con Merino Moraga, Pablo Andrés.

Los cargos presentados contra el usuario Pablo Andrés Merino Moraga, han sido basados bajo dos legislaciones vigentes chilenas. La primera de ellas en la Ley General de Telecomunicaciones y segunda la Ley 19.223, artículo 1°. El primer artículo de la mencionada normativa, dice “e*l que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento”* (Nacional, 1993)*.* De acuerdo a lo indicado en este artículo indica que toda mala utilización que fuese realizada con dolo, que provoque la disponibilidad de un sistema de información, podrá ser acusado de infringir la ley bajo el artículo mencionado.

De acuerdo a lo anterior, en este caso, Pablo Merino (imputado), es acusado de vender tarjetas modificadas por un programa obtenido de forma gratuita desde internet. Esta pieza de software, no ha sido programada por él, sino que por terceros que lo han desarrollado, con el fin de adulterar las tarjetas de codificación para receptores satelitales. Consiente de la finalidad del aplicativo, el imputado la utiliza en conocimiento del resultado de la utilización esta, lo cual es utilizado para obtener un beneficio propio.

* Nombre del caso*: “Sky Chile CPA con Merino Moraga, Pablo Andrés”*
* Cargos formulados*: “Venta de tarjetas de codificación para receptores de señal satelital modificadas para obtener acceso a dichos canales sin pagar a sus operadores.*

*Se formulan cargos contenidos en la Ley General de Telecomunicaciones, como infracción al artículo 1° de la Ley N° 19.223, al modificar el funcionamiento del sistema de tratamiento de información”.* (Chile P. J., 2012).

En el fallo otorgado por la Corte Suprema favoreció al imputado. El juez dictaminó que la utilización del programa no configuraba el delito descrito en artículo 1° de la Ley 19.223, dado que este aplicativo no fue desarrollado por el acusado, sino que obtenido de forma gratuita desde internet. Para mayor información del caso estudiado ver Anexo F.

### Polincay Export y Comercial Polincay Ltda. con Pérez Rodríguez

Los cargos presentados contra el usuario Pérez Rodríguez, han sido basados bajo el 2° artículo de la Ley 19.223. El segundo artículo de la mencionada normativa, dice “*El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él”* (Nacional, 1993)*.* Ahora bien, lo indicado en este artículo indica el que realice un acto doloso, que provoque que la confidencialidad de los datos contenidos un sistema de información, podrá ser acusado de infringir la ley bajo el artículo mencionado.

De acuerdo a lo anterior, en este caso, Pérez Rodríguez (acusado), es acusado de abusar de la confianza de su jefe para obtener las contraseñas de su correo electrónico y reenviar correos electrónicos con información confidencial de la empresa. Estos correos pudieron haber contenido información sensible de los negocios de la empresa, como también pudieron ser correos personales que la jefatura haya contenido en su casilla de correo, lo que hace pensar que pudo existir una infracción a la ley de protección de datos de carácter personal.

Sin embargo, a pesar que al acusado se le atribuyeron cargos bajo el artículo segundo de la ley de delitos informáticos, cabe pensar, el cómo se adquirió la contraseña. Bajo esta duda, cabe destacar que el sujeto perpetrador del ilícito pudo utilizar programas de espionaje para obtener la contraseña, como también de un descuido de la víctima, que la pudo dejar escrita en algún lugar o simplemente bajo algún tipo de circunstancia la víctima se la confió al acusado. Todas estas interrogantes logran ser válidas, ya que el artículo segundo habla obtención, del apoderamiento, usar o conocer información de un sistema informático, entonces la duda mayor es, como la víctima entra en la categoría de sistema de tratamiento de información.

* Nombre del caso*: “Polincay Export y Comercial Polincay Ltda. con Pérez Rodríguez, Raúl Ignacio”*
* Cargos formulados: “*Obtención de la contraseña de acceso al correo electrónico de su jefe, a fin de acceder al contenido de su computador.*

*El imputado cometió un abuso de confianza, reenviando otros correos del afectado a cuentas externas para obtener información acerca de su empleador y sus negocios*.”. (Chile P. J., 2012).

La Corte Suprema, conociendo de una casación en el fondo a la sentencia que absolvía al imputado, se pregunta respecto de la extensión de la palabra indebida en el artículo 2° de la ley. Esta resuelve que la intromisión no fue indebida, puesto que existió la autorización y consentimiento, lo que establece responsabilidad directamente sobre la víctima por haber puesto en peligro sus propios datos confidenciales. Para mayor información del caso estudiado ver Anexo F.

De acuerdo a lo expuesto en los casos, se aprecia que las infracciones denunciadas por las víctimas, han sido enjuiciadas por el artículo 1° y 2° de la Ley 19.223 (Nacional, 1993). Se aprecia una interpretación vaga y/o una falta de conocimiento de la normativa, tanto por los jueces como por parte de la fiscalía, en donde la expresión “*el que maliciosamente*” y “*el que con ánimo de apoderarse*”, ha sido causal de discordia para que los casos no hayan podido ser enjuiciados de forma correcta. Estas expresiones indican que debe existir un *dolo* en la acción realizada por el individuo activo sobre el pasivo. La problemática en los enjuiciamientos de los incidentes informáticos, es la verificación del *dolo* sobre la acción que se llevó a cabo, la demostración de la existencia de una intención específica sobre el incidente ocurrido.

## CONVENIO DE BUDAPEST EN CASOS APLICADOS

A continuación, se han desarrollado los casos expuestos anteriormente, mediante la utilización de los artículos del tratado de Budapest. La aplicación del convenio en los casos descritos, es para demostrar que el desarrollo de este para obtener un fallo favorable para la víctima. Se expondrá la justificación de la utilización de los artículos del convenio de Budapest por los cuales se han desarrollado los casos.

### Convenio de Budapest e hipermercado Curicó

Como se habría expuesto anteriormente, el caso de hipermercado Curicó y María de las Nieves, se encontraba sujeto al fallo bajo el primer artículo de la Ley 19.223, el cual fue a favor de la acusada. Los hechos evidenciados para sancionar a la acusada, están relacionados con el aprovechamiento de forma dolosa de un aplicativo que se encontraba con fallas en su programación, lo que fue detectado por la acusada. Ver Anexo F. Ahora este caso, será desarrollado bajo los artículos del Convenio Budapest, como se muestra a continuación:

Artículo Convenio de Budapest:

* Artículo 8, fraude informático. Se declara que son los actos que causen un perjuicio patrimonial mediante la introducción, alteración, borrado de datos informáticos, como también las acciones que alteren el funcionamiento de un sistema de información con la finalidad de obtener beneficios económicos de forma ilegal.
* Para una mayor descripción del artículo ver Anexo G.

Conclusiones:

* Mediante la aplicación del artículo 8 del tratado de Budapest, en el caso “Hipermercado Curicó Limitada con Lizama Ponce, María de las Nieves y otros”, se hubiera podido sancionar de forma correcta. La aplicación del artículo, el que tipifica un acto deliberado que fue utilizado para beneficio del acusado, como cita el primer párrafo del mencionado artículo y en segundo lugar, se habla de una interferencia del funcionamiento del aplicativo para cargar las tarjetas, lo que se traduce, en que este acto lo cometió con conciencia del mal funcionamiento, es decir, de forma dolosa.

A su misma vez, como se dijo anteriormente, el acto lo desarrollo para su beneficio propio. Este actuar, se traduce en un perjuicio para el patrimonio del dueño del hipermercado.

### Convenio de Budapest y Sky Chile

El caso de Sky Chile CPA con Merino Moraga, Pablo Andrés, se encontraba sujeto al fallo bajo el primer artículo de la Ley 19.223, el cual fue a favor del acusado. Los hechos evidenciados para sancionar al acusado, están relacionados con la modificación de las tarjetas de los decodificadores de la televisión satelital por medio de un aplicativo descargado de forma gratuita. Este aplicativo es desarrollado por terceros, los que han puesto a disposición de los usuarios esta pieza de software.

El acusado para llevar a cabo el ilícito, debió estudiar y aprender cómo utilizar el aplicativo. Una vez que el acusado obtuvo los conocimientos necesarios para la utilización del software, pudo llevar a cabo las modificaciones a las tarjetas de los decodificadores, los que una vez con su cambio desarrollado pudo realizar acciones en su beneficio propio, llevando a cabo un perjuicio económico a Sky Chile. Ver Anexo F. Ahora este caso, será desarrollado bajo los artículos del Convenio Budapest, como se muestra a continuación:

Artículo Convenio de Budapest:

* Artículo 6°, Abuso de los dispositivos. Será considerado bajo esta tipificación todo acto realizado por medio de un dispositivo informático, programas y/o contraseñas adquiridos, importados que permitan obtener acceso a un sistema de información con el fin de obtener un beneficio propio
* Artículo 8°, Fraude informático. Se declara que son los actos que causen un perjuicio patrimonial mediante la introducción, alteración, borrado de datos informáticos, como también las acciones que alteren el funcionamiento de un sistema de información con la finalidad de obtener beneficios económicos de forma ilegal.
* Para una mayor descripción del artículo ver Anexo G.

Conclusiones:

* Mediante la aplicación de los artículos 6° y 8° del tratado de Budapest en el caso “Sky Chile CPA con Merino Moraga, Pablo Andrés”, se hubiera podido sancionar de forma correcta mediante la utilización de ambos artículos. Primero, mediante el artículo 6, el cual tipifica la obtención de cualquier dispositivo o pieza de software el cual sea utilizado para fines ilícitos, con lo que se deduce, que la comisión de un acto delictual sin importar el origen de los dispositivos y/o programas computacionales utilizados.

Ahora desde el punto de vista del artículo 8° del tratado, el caso se podría sancionar mediante este artículo. De acuerdo a lo anterior, esta acción trajo consigo un perjuicio patrimonial para otra persona, en este caso, para la empresa Sky Chile CPA, en conjunto con la anterior tipificación, también este ilícito cae en la figura descrita en el apartado a), que indica cualquier introducción, alteración, borrado o supresión de datos informáticos.

En conclusión, el dictamen, puede llevarse a cabo mediante los dos artículos aplicados. Es decir, cado uno hubiera sancionado un acto distinto del caso, o sea, dejando al artículo 6° sancionar la obtención de una aplicación para fines ilícitos y por último el artículo 8° que tipifica la alteración de datos informáticos de un dispositivo y también con la obtención de un lucro personal y el perjuicio económico percibido por la empresa Sky Chile. Por último también hubieran sido agravante una del otro, lo que hubiera transformado la sentencia en una sumatoria de penas.

## CONCLUSIONES

A modo de conclusión, durante el desarrollo del capítulo se desarrollaron temas de gran relevancia como las leyes contenidas en el Convenio de Budapest y los derechos fundamentales. Dentro del tratado, se encuentran los artículos 9 y 10, que describen los actos que atentan contra la pornografía infantil y la propiedad intelectual. Actualmente la legislación nacional cuenta con dos leyes específicas para estos actos, que son la Ley 20.526 que aborda los delitos contra la pornografía infantil y la Ley 17.336 que enmarca los ilícitos contra la propiedad intelectual. Ahora bien, si Chile, decidiera adherirse al Convenio de Budapest, podría hacerlo mediante la reserva de estos artículos, dejando indexado los artículos a estas dos leyes.

Por otra parte, se habló sobre los derechos fundamentales, en especial atención al artículo 19 número cuatro. Este artículo habla sobre el derecho a la privacidad y la honra de la vida del ciudadano chileno. El Convenio de Budapest, habla sobre la retención y entrega de datos de personas a los Estados partes en caso que lo requiera una investigación desarrollada por el país adherido. Chile por su parte, dentro de la Constitución política se describe, que únicamente se podrá hacer invadir dicha privacidad en el caso que la seguridad nacional se vea involucrada. Dicho lo anterior, es válido cuestionar la adherencia al Convenio de Budapest, en caso que esta se realice sin la reserva del artículo 29, que hace referencia a *la* conservación rápida de datos informáticos almacenados, cuando este solicita la entrega de información de navegación del usuario a terceros y en Chile, esta solicitud será válida si existe compromiso nacional.

También otro punto destacado, fue el alto índice de delitos investigados por la infracción a la Ley N° 19.223 y el drástico descenso en las detenciones realizadas por la Policía de Investigaciones de Chile (en adelante PDI) por la razón descrita anteriormente. Las cifras observadas en la tabla 4.2, indican que el ciudadano chileno o las empresas chilenas, realizan denuncias ante la autoridad, porque creen que han sido víctimas de un delito informático (de acuerdo a lo descrito en los artículos de la ley de delitos informáticos). Sin embargo, cuando estas denuncias son investigadas por la PDI, puede ser que se encuentren con un escenario poco favorable para ellos, como por ejemplo, el acto denunciado no se configura con la norma vigente de delitos informáticos nacional, también es posible que la persona que cometió el ilícito no se encuentre domiciliado en el país, lo que haría imposible poder tomar acciones ante esto. Por otro lado, en el caso que la PDI, dentro de su investigación, encuentre que el delito está tipificado en la normativa nacional y el delincuente se encuentre dentro del territorio nacional, este podrá ser llevado a los tribunales para realizar su enjuiciamiento por los actos denunciados. Ahora bien, es correcto preguntar si el juez o el fiscal que llevan la causa, tienen los conocimientos necesarios para entender el funcionamiento del acto malicioso y con ello entregar una correcta sanción por la infracción cometida.

# EVALUACIÓN Y ANÁLISIS DE RESULTADOS

En este capítulo se expone la evaluación y un análisis de los resultados obtenidos en el presente trabajo de tesis. Primero se analizará el significado de llevar a cabo la adherencia al Convenio de Budapest, o sea, se analizarán los puntos clave de este proyecto de ley. Por último se dará a conocer una opinión sobre la capacidad de juzgar a los denunciados bajo la ley de delitos informáticos.

## CONSTITUCIÓN DE CHILE Y EL TRATADO

El proyecto de ley chileno sobre la adhesión al Convenio de Budapest se verá enfrentado a una imposición establecida que atenta contra el espíritu de este. Una de las razones más grandes para adherirse a este tratado es la cooperar internacionalmente entre estados miembros, contra la comisión de delitos cometidos con el uso de las tecnologías de información. El proyecto de ley indica que se deberá realizar mediante la reserva de cinco artículos, donde se encuentra incluido el artículo 29 de c*onservación rápida de datos informáticos almacenados*, que para el entender del autor del presente estudio, es uno de los más importantes dentro de la redacción del Convenio de Budapest sobre la Ciberdelincuencia.

Ahora bien, el artículo 29, habla sobre la conservación de los datos informáticos de los usuarios. En Chile, la razón por la cual se ha establecido la reserva de este artículo es por la existencia del artículo 19 número cuatro de la Constitución Política de Chile, que dice “e*l respeto y protección a la vida privada y a la honra de la persona y su familia*”. De acuerdo a lo expuesto por el mencionado artículo de la Constitución chilena, la vida privada deberá ser considerada como un derecho. Este acto se define como la posición de una persona que se encuentre libre de intromisiones o propagaciones de sus pensamientos y/o conductas que pertenezcan a su interioridad corporal y psicológica o a las relaciones que mantiene o ha mantenido con otros, o sea, consiste en la inexistencia de intromisiones o difusiones cognoscitivas, limitando así la privacidad del derecho a la honra, a la imagen, a la integridad física y la libertad para adoptar decisiones personales.

De acuerdo a lo anterior, la situación de Chile ante el proyecto de ley que inicia el proceso de adhesión al Convenio de Budapest sería un acto que dejaría sin alma a un tratado internacional que es necesaria su cooperación entre todos los miembros. Si bien es cierto, el tratado permite a los miembros a reservar artículos, pero también Chile ha incluido los artículos 4, 6, 9 y 22, sin olvidar el 29, dentro de su reserva. En las descripciones de los artículos reservados, se han encontrado las siguientes descripciones:

1. Artículo 4, como ataques a la integridad de los datos.
2. Artículo 6, abuso de los dispositivos.
3. Artículo 9, delitos relacionados con la pornografía infantil.
4. Artículo 22, jurisdicción.
5. Artículo 29, conservación rápida de datos informáticos almacenados.

En los artículos reservados se encuentran delitos que han sido tipificados dentro del convenio. Estos ilícitos son el artículo 4, 6 y 9, los cuales no se encuentran identificados dentro de la legislación chilena a excepción del artículo 4 y 9, que sanciona los delitos relacionados contra la integridad de los datos y la pornografía infantil, mientras que los de abuso de dispositivos no ha sido encontrado dentro de la ley nacional. Junto con lo anterior, se puede encontrar la figura de ataque a la integridad de los datos, lo que se encuentra contemplado en la Ley 19.223 de delitos informáticos, pero esto no es clara su tipificación, ya que para obtener esta figura, se debe conjugar dos artículos de la presente ley, el 1 y 3, que se identifica el ilícito de sabotaje informático, el que comprende las conductas que interfieren con el correcto funcionamiento de los componentes (*hardware o software*) y los datos contenidos en estos.

Ahora bien, si el proyecto de ley enviado al Honorable Cámara del Senado chileno, para adherir a Chile al convenio es aceptado, puede ser que se estén cometiendo acciones sin pensar en el futuro. Si bien es cierto, la adhesión al tratado, es un tema novedoso para la legislación chilena, por que podrá ingresar a un círculo de países desarrollados, en donde ellos comparten información de sus ciudadanos para solucionar, mientras que Chile en la posición que ha planteado este proceso, no realizará. Ante esto, se pueden plantear dos posibles soluciones, la primera de ellas, es que Chile pueda modificar este proyecto de ley enviado y replantee la forma de realizar la adhesión, dejando con reservas los artículos relacionados a los delitos de pornografía infantil y los que atentan contra la propiedad intelectual, donde Chile, cuenta con leyes dedicadas específicamente para cada uno de estos ilícitos descritos en el Convenio de Budapest.

Por otro lado, otra solución es la de poder reformular la actual ley de delitos informáticos, teniendo como base el Convenio de Budapest. Con este punto se pueden esclarecer las conductas atípicas que son sancionadas por un tratado internacional, dejando sin efecto la cooperación internacional y la de conservar datos de los usuarios los que puedan ser entregados a otros países miembros, significando un amplio abanico de delitos informáticos que podrán ser sancionados por una ley nacional.

## CAPACIDAD DE JUZGAR BAJO UNA LEY SIN CONOCIMIENTO

De acuerdo a los datos entregados por la policía de investigaciones en sus estadísticas de delitos perseguidos y los sancionados, se concluye que no todos los actos investigados han logrado ser condenados. De acuerdo a esto se puede deducir por tres grandes trabas, que de acuerdo al criterio expuesto por el presentador del trabajo investigativo han sido fundamentales. El primero de ellos es la pobre calidad de la actual ley de delitos informáticos chilena. Se desarrolla calidad como la inexistencia de figuras penales por las cuales han sido denunciados los delitos investigados. La segunda, es la capacidad de poder juzgar o dictaminar sentencias por parte de los jueces y/o fiscales que han llevado las causas. Por último la tercera razón, es la falta de cuidado que tienen los usuarios con sus datos personales.

Para poder ahondar un poco más es las ideas expuestas anteriormente, se han desarrollado en conformidad al criterio del presentador del trabajo investigativo, exponiendo sus puntos de vista a las problemáticas planteadas. En primera instancia se desarrolló la idea de una pobre calidad de la ley de delitos informáticos chilena. Se indica como pobre, por la razón que esta ley data del año 1993, cuando las tecnologías, el uso de las computadoras, el internet, prácticamente no existían en Chile, únicamente tenían estos “lujos”, las empresas que existían en el país en aquellos años. Junto con lo anterior, dicha normativa, estaba orientada a la comisión del ilícito que atentaba contra el computador o el sistema de información, nunca fue orientada a la información contenida por estos, razón por lo cual, esta norma se encuentra casi obsoleta, si es que esta ya no se encuentra en esa calidad. La segunda idea expuesta, se desarrolla bajo la capacidad de poder juzgar o dictaminar sentencias. Bajo este punto de vista, los jueces y fiscales se encuentran en una gran disyuntiva, la cual es, quien sabe más o quien interpreta mejor la ley de delitos informáticos. Estas autoridades chilenas no cuentan con un criterio unificado, el cual les ayude a poder generar acciones y pensamientos similares para desarrollar este tipo de juicio. Si bien es verdad, que ellos son personas distintas, con pensamientos distintos y vidas diferentes, pero eso no es un impedimento para tener los conocimientos necesarios para estas ocasiones, razón por la cual, es mi deber como investigador el recomendar que se capaciten en cursos y/o capacitaciones relacionados con la materia en estudio, la asistencia a seminarios, con los cuales podrán encontrar una base igualitaria para ambas autoridades.

Por último y para criterio del presentador, el punto más importante, el cual afecta directamente al usuario. Se marca como el más importante, porque es el ciudadano quien debe tener resguardo con sus datos personales, con sus tarjetas de crédito, es él quien debe denunciar estos ilícitos. En relación a la persona, la ciudadanía ha sido muy pasiva ante estos actos, pensando que jamás le sucederá un hurto de información, confiando ciegamente en sitios web donde podrán ser víctimas de phishing u otra acción que permita hurtar sus datos personales, bancarios y por esta razón los delincuentes han aprovechado esta incredulidad y cometen los actos ilícitos. También es verdad, que existe una falencia en la legislación nacional que compete a los delitos informáticos, pero no hay que olvidar, que el usuario es el principal actor en todo esto y por ende, debe tener una participación más activa y ser más cuidadoso con sus datos.

Si bien es cierto, como se indicó anteriormente, el usuario debe ser más cuidadoso con sus datos, también el Gobierno chileno, tiene que ser partícipe de esto. La creación de leyes, campañas u otro tipo de iniciativa para apoyar y educar al usuario en cuanto a estos cuidados. Este apoyo o educación, debe realizarse al ciudadano chileno, porque no todos tendrán un acceso o contarán con recursos para poder ingresar a cursos o capacitaciones que hablen del tema de seguridad de datos, junto con esta razón, la cual es muy válida, la creación de nuevas leyes, que protejan más al usuario y que entreguen mayores multas a las empresas que venden los datos personales a otras.

# CONCLUSIONES

En este capítulo se presentan las conclusiones a partir de los resultados obtenidos a lo largo de esta investigación los cuales se presentan en tres secciones. En primer lugar se plantean las conclusiones obtenidas a partir de los resultados de la comparación entre la legislación nacional en materia de delitos informáticos y la de un país adherido al Convenio de Budapest, junto con la conclusión del análisis de la situación en que Chile modifique la Ley N° 19.223 junto con algunas reflexiones personales. En la segunda sección, describe los antecedentes que sostienen el cumplimiento de los objetivos planteados en el inicio del presente trabajo de tesis. Finalmente en la tercera sección se plantean algunos trabajos futuros a los que podría dar origen la línea de esta investigación.

## CONCLUSIONES GENERALES

No cabe duda que Chile se encuentra ante un escenario complejo ante los sucesos ilícitos que son cometidos por medio de las tecnologías de información, los llamados delitos informáticos. Ante esto, Chile cuenta con la Ley 19.223 de delitos informáticos que data del año 1993, redactada para tiempos cuando las tecnologías y el acceso a internet no se encontraban masificados como hoy en día. Con el pasar de los años, las tecnologías tuvieron un desarrollo y una penetración en la ciudadanía que se desarrolló a gran velocidad. Esto permitió que los chilenos pudieran tener acceso a estos recursos tecnológicos los que han sido utilizados en sus quehaceres diarios, sus trabajos, para diversión o para uso familiar y dando también origen el acceso a internet. Este acceso a las tecnologías originó a una nueva era, que en conjunto con la globalización y el tráfico de información entre los usuarios, gobiernos y empresas, dieron lugar a actividades que buscaban obtener un aprovechamiento de las tecnologías de información para obtener un beneficio propio a costa de acciones ilícitas.

La complejidad de la red de redes, el internet, hace que la persecución de los delitos informáticos sea muy compleja. Esta situación hace posible que se encuentren casos en los que el acto perseguido sea un ilícito en un país, mientras que en otro no lo sea, o bien que la sentencia condenatoria de un país quede sin efectos porque el otro país no ejecute una norma penal extranjera. En este tipo de situación se encuentra Chile, porque la ley vigente que tipifica estos actos, no se ajusta a los actos que atentan contra el ciudadano chileno, como el *hacking*, *phishing* por nombrar algunos.

Gracias a la problemática planteada por el avance de las tecnologías, los delitos informáticos, se elaboraron cuatro proyectos para modificar la normativa vigente que sanciona los delitos informáticos. En la Honorable Cámara de Diputados de Chile se tramitaron los proyectos de ley 2974-19, 7090-07, 9998-07 y el 10145-07, desarrollados entre los años 2002 y 2015, siendo archivados o se encuentran en tramitación en el Congreso Nacional. Ahora bien, durante el año 2009 se presentó el Decreto N° 3265, que dictaminó la creación del Comité Interministerial sobre Ciberseguridad en Chile, que tenía como finalidad coordinar los requerimientos y las acciones conducentes a la adhesión de Chile a la Convención sobre Ciber Delitos del Consejo de Europa, acciones que no se concretaron. Durante el año 2015, se elaboró el Decreto Supremo N° 533, que insta la creación de una política de ciberseguridad para Chile y marca el hito para realizar la adhesión al Convenio de Budapest.

Durante la promulgación del Decreto Supremo 533, se plantea realizar la adhesión al Convenio de Budapest mediante la reserva de cinco de sus artículos. Los artículos 4, 6, 9, 22 y 29, según los legisladores, no se adecuan a la normativa nacional. Dentro de la normativa nacional se encuentra la Ley 20.526 *que sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil*, la cual se encuentra contemplada en el artículo 9 del Convenio de Budapest, que tipifica los delitos relacionados con la pornografía infantil, también junto con el artículo anterior, se puede destacar el artículo 10, que tipifica los delitos relacionados con infracciones de la propiedad intelectual y de derechos afines, para el cual se puede encontrar contenido dentro de la Ley 17.336, *sobre propiedad intelectual*.

Analizando el proyecto de ley sobre la adherencia de Chile al Convenio de Budapest, este podría generar ambigüedad, vacíos legales y vulneración a los derechos descritos en la constitución política. Dentro del La presentación de una serie de artículos proyecto de ley presentado, indica reserva artículos del tratado, los jueces podrían perder la capacidad de sanción sobre los delitos cometidos por medios informáticos, porque no tendrían la capacidad de sancionar la incorrecta utilización de dispositivos, los que han podido ser obtenidos por distintos medios, generando nuevamente una ley ambigua, donde este tipo de actos no se encuentre tipificado, siguiendo la misma línea de lo existente en el país.

Ahora bien, nos queda preguntar cuál será la mejor solución para Chile. Será la de llevar a cabo la adhesión al Convenio de Budapest, o de realizar una modificación a la ley de delitos informáticos actual, sin tener la necesidad de llevar a cabo la adherencia al tratado, lo cual significaría tipificar las nuevas acciones ilícitas que han sido identificadas y también el de enfrentar un gran desafío, el de llevar a cabo una unificación de criterios entre los jueces, fiscales y policías locales, para poder sancionar de forma correcta las acciones denunciadas.

## CUMPLIMIENTO DE LOS OBJETIVOS

OE1: Para el desarrollo del objetivo específico número uno, se expusieron los conceptos planteados en el capítulo 2. En este capítulo se expusieron los conceptos teóricos relevantes del presente trabajo de tesis. Primero se analizó el concepto de ciberdelincuencia, detallando los tipos de ilícitos que actualmente se encuentran vigentes según las Naciones Unidas (*UN*). Seguido de esto se desarrolló una definición del Convenio de Budapest sobre la Ciberdelincuencia. Para dar continuación al tema relevante al estudio presentado, se expuso el significado de la ciberdelincuencia en Chile, seguido de la descripción de la Ley 19.223 de Delitos Informáticos, junto con ello se describieron las normativas chilenas, en donde se desarrollaron los proyectos de ley para la actualización de la actual ley de delitos informáticos chilena, terminando con la explicación del Decreto N° 3265 que crea Comité Interministerial sobre Ciberseguridad.

OE2: Para el desarrollo del segundo objetivo específico, se realizó el análisis de brecha entre la legislación chilena y la de un país adherido al Convenio de Budapest sobre la Ciberdelincuencia. Este punto se desarrolló en el capítulo 3, donde se realizó un estudio comparativo de legislaciones vigentes en los países Latinoamericanos de Argentina, Brasil, Chile, Colombia, Perú, Puerto Rico, República Dominicana, Uruguay, Venezuela. El cumplimiento de este objetivo se dio con la comparación de Chile y de la República Dominicana. Se detectó una importante brecha en el marco legal de cada país, como queda demostrado en el Tabla 3.1.

OE3: Para el desarrollo del tercer objetivo específico, se ha identificado ventajas y desventajas de la adherencia al Convenio de Budapest y en la actualización a la Ley N° 19.223. Este punto se desarrolló en el capítulo 5, apartado 5.1, mediante el resultado del estudio, se identificaron las desventajas de la adherencia al convenio, no existiendo ventajas ante la adherencia al tratado. Esta conclusión se basa en la existencia de la reserva de cinco artículos indicados por el Gobierno chileno, especialmente del artículo 29 del tratado, que habla sobre la conservación rápida de datos informáticos almacenados, también se ha indicado que existen artículos del tratado, que sí podrían ser reservados, el artículo 9 que habla sobre delitos relacionados con la pornografía infantil y el artículo 10, que habla sobre los delitos relacionados con infracciones de la propiedad intelectual y de derecho afines, los que cuentan con leyes especiales y dedicadas para estos dos ilícitos.

OE4: El desarrollo del objetivo específico 4, se generaron tres casos de estudios. El desarrollo de este punto se llevó a cabo en el capítulo 4, apartado 4.4 donde se describieron los casos a desarrollar, mostrando los cargos formulados por la policía y fiscales a cargo de la investigación y también los dictámenes entregados por los jueces que llevaron las distintas causas desarrolladas. Por último en el apartado 4.5, se desarrollaron los casos mediante la aplicación de los artículos del Convenio de Budapest sobre los casos desarrollados bajo la Ley 19.223 de Delitos Informáticos. Junto con lo anterior, se apreció la aplicación y criterios utilizados por la Corte Suprema y Corte de Apelaciones al momento de sancionar los incidentes cometidos en Chile. En los casos se evidenció, que hay una inexistencia de tipificaciones, las cueles generan una ambigüedad cuando se interpretan los artículos de la Ley 19.223. Cuando se aplicó el Convenio de Budapest sobre la Ciberdelincuencia a cabalidad, sin obviar artículos como lo han propuesto desde el Gobierno, se ha obtenido resoluciones a partir de la interpretación de los incidentes tipificados en el tratado.

OE5: El desarrollo del objetivo específico 5 se generaron las recomendaciones de llevar a cabo concientizaciones sobre temas de seguridad de los datos personales a los usuarios. Este punto fue desarrollado en el capítulo 5, en donde se propone generar políticas públicas que incentiven a la educación de la ciudadanía en cuanto al cuidado que deben tener sobre sus datos personales. La finalidad de la creación de estas medidas o ayudas para los usuarios, es minimizar el alto índice de denuncias por infracción a la Ley 19.223 de delitos informáticos que recibe la Policía de Investigaciones de Chile, lo que ha quedado demostrado en el capítulo 4, apartado 4.3, donde se evidenció el elevado porcentaje de denuncias tanto por el delito de espionaje y sabotaje informático, lo que ayudaría a minimizar la necesidad de realizar una actualización al sistema legal en materia de delitos informáticos.

## TRABAJOS FUTUROS

El estudio ejecutado en base al proyecto de ley que hace referencia a la falta de una ley acorde a los tiempos modernos para los delitos informáticos que nos acechan hoy en día. Ante esto, el Gobierno de Chile ha planteado una posible adhesión al Convenio de Budapest sobre la Ciberdelincuencia. Por otro lado tenemos la Ley N° 19.223 de delitos informáticos, a la cual se le han presentado 4 proyectos de ley para realizar su modificación.

Para dar un mejor entendimiento a la problemática, se realizó un estudio comparativo, entre países pertenecientes a Latinoamérica. En esta comparación se identificaron los países que cuentan con legislaciones que tipifican los delitos informáticos. Junto con lo anterior, se identificaron los actos ilícitos que son sancionados de acuerdo a lo establecido en el Convenio de Budapest. De acuerdo a los resultados obtenidos se pudo apreciar que a nivel latinoamericano la existencia de falencias en el desarrollo legislativo para sancionar estos actos, mientras tanto en otros países, como en el caso de República Dominica, contemplan una legislación acorde a los tiempos modernos.

Bajo esta temática, dado que Chile, no cuenta con una legislación actualizada. Se plantea el desarrollo de herramientas y/o manuales que permita tener un claro entendimiento del convenio. Este desarrollo, debe ser contar con el conocimiento especializado en la materia, pero a su vez deberá ser utilizada por abogados, jueces, magistrados y también usuarios que no cuenten con la experiencia necesaria, como ingenieros u otros que quieran entender el funcionamiento y aplicación del tratado. Estas herramientas, deberán ayudar a realizar concientización y sensibilización en la materia de ciberdelincuencia, aplicando mejores prácticas de cómo hacer valer los derechos que se encuentran estampados en el tratado.

# REFERENCIAS BIBLIOGRÁFICAS

Argentino, H. s. (2008). *Modificacion codigo penal de Argentina.* Obtenido de http://www.oas.org/juridico/PDFs/arg\_ley26388.pdf

Brasileña, P. d. (2012). *Asuntos jurídicos*. Obtenido de http://www.penal.org/sites/default/files/files/RM-4.pdf

Caribe, T. d. (2014). Obtenido de https://www.symantec.com/content/es/mx/enterprise/other\_resources/b-cyber-security-trends-report-lamc.pdf

CERN. (2013). *Organización Europea para la Investigación Nuclear*. Obtenido de http://www.europapress.es/portaltic/internet/noticia-cern-habilita-primera-url-historia-conmemorar-world-wide-web-20130430161046.html

Chile, C. d. (2002). *Camara de Diputados de Chile*. Obtenido de https://www.camara.cl/pley/pley\_buscador.aspx

Chile, C. d. (2011). *Cámada de Diputados*. Obtenido de https://www.camara.cl/prensa/noticias\_detalle.aspx?prmid=42517

Chile, C. G. (2016). *CSIRT - Gobierno de Chile*. Obtenido de http://www.csirt.gob.cl/

Chile, C. n. (1970). *Ley 17.336 Propiedad intelectual.* Obtenido de http://www.leychile.cl/Navegar?idNorma=28933

Chile, C. P. (2005). *Constitución Política de la República de Chile.* Obtenido de http://bcn.cl/1uva9

Chile, P. J. (2012). *Sistema Informático Corte Suprema*. Obtenido de http://suprema.poderjudicial.cl/SITSUPPORWEB/InicioAplicacion.do

Cibernéticos, U. I. (2012). *Delitos Cibernéticos - Internet Seguro*. Obtenido de http://internetseguro.pr.gov/delitosciberneticos/

Colombia, C. d. (2008). *Ley 1236 de 2008 - Reforma Penal - Delitos de abuso sexual*. Obtenido de https://www.oas.org/dil/esp/Ley\_1236\_de\_2008\_Colombia.pdf

Comunicaciones, M. d. (2009). *Ley 1273 de 2009*. Obtenido de http://www.mintic.gov.co/portal/604/w3-article-3705.html

Congreso, B. d. (2011). *Sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil.* Obtenido de http://web.uchile.cl/archivos/derecho/CEDI/Normativa/Ley%2020.526%20Sanciona%20el%20Acoso%20Sexual%20de%20Menores,%20la%20Pornograf%EDa%20Infantil%20Virtual%20y%20la%20Posesi%F3n%20de%20Material%20Pornogr%E1fico%20Infantil.pdf

Delito, O. d. (2005). *United Nations Office on Drugs and Crime.* Obtenido de http://www.unis.unvienna.org/pdf/05-82113\_S\_6\_pr\_SFS.pdf

Derecho, C. d. (2012). *Revista Chilena de Derecho y Tecnologia*. Obtenido de http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629

Dominicana, M. d. (2013). *Adhesión Convenio de Budapest.* Obtenido de http://enlacecongreso.mirex.gov.do/ecc/Lists/Instrumentos%20Internacionales/Attachments/3207/Convencion%20de%20Ciberdelincuencia0001.pdf

Dominicano, S. y. (2016). *Portal Oficial del Estado Dominicano, Seguridad y Delito Electrónico*. Obtenido de http://www.gob.do/index.php/politicas/2014-12-16-20-56-34/politicas-para-el-buen-gobierno/delito-electronico

Dominicano, S. y.-P. (2016). *Portal Oficial del Estado Dominicano, Seguridad y Delito Electrónico*. Obtenido de http://www.gob.do/index.php/politicas/2014-12-16-20-56-34/politicas-para-el-buen-gobierno/delito-electronico

Egaña, J. L. (2003). *Derecho Constitucional Chileno Tomo II.* Santiago: Ediciones Universidad Católica de Chile.

Estrategia, D. l. (Junio de 2016). Obtenido de http://www.estrategia.cl/8309/Titulo

Europe, C. o. (Noviembre de 2001). *Convenio sobre la Ciberdelincuencia.* Obtenido de Convenio sobre la Ciberdelincuencia: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS\_185\_spanish.PDF

Europe, C. o. (2001). *Council of Europe*. Obtenido de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

García, C. A. (2004). *Las Grandes Divisiones del Derecho.* Obtenido de http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/242/art/art1.pdf

Glossary Ciberdelincuencia, C. d. (2001). *Glossary.* Obtenido de http://www.coe.int/en/web/conventions/glossary

Guatemala, U. S. (2014). Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica. *Seguridad de la Información*, 165 - 167.

Huerta, M., & Libano, C. (1998). Delitos Informáticos. En C. L. Marcelo Huerta. Santiago: Jurídica ConoSur.

Informatico, C. d. (2014). *Revista Chilena de Derecho y Tecnologia*. Obtenido de http://www.rchdt.uchile.cl/index.php/RCHDT/article/viewFile/32220/34154

Interior, M. d. (Diciembre de 2009). *Ministerio del Interior.* Obtenido de http://bcn.cl/1wbya

Interior, M. d. (Diciembre de 2015). Obtenido de http://bcn.cl/1wbya

Isaca. (2007). *Isaca*. Obtenido de http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf?regnum=337307

Judicial, P. (2016). Obtenido de http://corte.poderjudicial.cl/SITCORTEPORWEB/

jurídica, S. c. (2012). *Reforma de la Sección VIII, Delitos Informáticos.* Obtenido de http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm\_texto\_completo.aspx?nValor1=1&nValor2=73583

Justicia, M. d. (2011). *Sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil*. Obtenido de http://bcn.cl/1v0ah

Kunz, A. y. (2005). Guía para estudiantes y tesistas. En A. y. KUNZ.

Legislativo, R. O.-P. (2009). *Ley N° 18.600 - Documento Electrónico y Firma Electrónica*. Obtenido de https://legislativo.parlamento.gub.uy/temporales/leytemp1143267.htm

Luis de la Corte Ibáñez, J. M. (2014). *Seguridad nacional, amenzas y respuestas.* Madrid: Editorial Empresarial .

Mercurio, E. (2014). *El Mercurio online*. Obtenido de http://impresa.elmercurio.com/pages/LUNHomepage.aspx?BodyID=3&dt=2014-10-24&dtB=2014-10-24&dtB=24-10-2014

Mexía, P. G. (2009). *Derecho Europeo de Internet.* La Coruña: Netbiblo.

Nacional, B. d. (diciembre de 1993). *Biblioteca del Congreso Nacional.* Obtenido de bcn.cl/1m196

Navigator, N. (2008). *Netscape Navigator*. Obtenido de https://es.wikipedia.org/wiki/Netscape\_Navigator

oficial, I. -C. (2004). *Ley N° 17815*. Obtenido de https://www.impo.com.uy/bases/leyes/17815-2004

Oiprodat. (2014). *Observatorio Iberoamericano de Proteccion de Datos*. Obtenido de http://oiprodat.com/2014/03/04/colombia-y-la-cooperacion-internacional-en-los-delitos-informaticos/

Penal, C. (2016). *Codigo Penal.* Obtenido de http://bcn.cl/1uvs0

Penal, C. P. (2016). *Codigo Procesal Penal.* Obtenido de http://bcn.cl/1uvvn

personal, P. d. (1999). *Protección de Datos de carácter personal*. Obtenido de http://bcn.cl/1uv2v

Perú, C. d. (2004). *Ley N° 28251.* Obtenido de http://comisionunidosvstrata.org/wp-content/uploads/2014/05/per-ley-28251.pdf

Peruana, C. d. (2000). *Ley N° 27309.* Obtenido de http://www.oas.org/juridico/spanish/cyb\_per\_ley\_27309.pdf

Peruano, C. (2005). *Ley contra el Spam.* Obtenido de http://www.inen.sld.pe/portal/documentos/pdf/normas\_legales/NUEVA\_leyes/2005/28042010\_LEY\_N\_28493.pdf

Presidencia, M. S. (1999). *Ministerio Secretaría General de la Presidencia*. Obtenido de http://bcn.cl/1uv2v

Presidencia, M. S. (2008). *Acceso a la Información Pública*. Obtenido de http://bcn.cl/1uuq2

Privacidad, D. d. (1999). *Derecho de la Privacidad*. Obtenido de http://bcn.cl/1uv2v

Pública, M. d. (2015). Obtenido de http://bcn.cl/1uwi4

Pública, M. d. (2015). *Ministerio del Interior y Seguridad Pública*. Obtenido de http://bcn.cl/1uwi4

Rodríguez, A. W. (2008). Diccionario Latín Jurídico, Locuciones latinas de aplicación jurídica actual. En A. W. RODRÍGUEZ.

Symantec. (abril de 2012). *Symantec.* Obtenido de https://www.symantec.com/content/es/mx/enterprise/threatreport/ISTR17-americas-spanish.pdf

Symantec, O. (2014). *Tendencias de seguridad cibernética en America Latina y el Caribe.* Obtenido de https://www.symantec.com/content/es/mx/enterprise/other\_resources/b-cyber-security-trends-report-lamc.pdf

Tecnología, D. d. (2016). *Departamento de Investigaciones y Crímenes de Alta Tecnología*. Obtenido de http://dicat.gob.do/

Tecnología, R. C. (Enero de 2012). Obtenido de http://www.revistas.uchile.cl/index.php/RCHDT/article/viewFile/24030/25629

Telecomunicaciones, M. d. (2005). *Ministerio de Transporte y Telecomunicaciones*. Obtenido de http://bcn.cl/1vvcl

telecomunicaciones, S. d. (2016). *Accesos a internet*. Obtenido de http://www.subtel.gob.cl/accesos-a-internet-llegan-a-131-millones-y-uso-de-smartphones-sigue-en-alza/

Unidas, N. (2000). *X Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.* Obtenido de http://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml

Uruguay, E. S. (2002). *Uso indebido de señales destinadas a ser recibidas en regimen de suscripción - Ley 17.520*. Obtenido de https://legislativo.parlamento.gub.uy/temporales/leytemp71619.htm

Uruguay, I. -N. (1933). *Código Penal N° 9155*. Obtenido de https://www.impo.com.uy/bases/codigo-penal/9155-1933

Venezuela, A. n. (2001). *Ley especial contra los delitos informáticos*. Obtenido de http://www.oas.org/juridico/spanish/mesicic3\_ven\_anexo18.pdf

# ANEXOS

**Anexo A. Países miembros del Consejo Europeo**

En la siguiente tabla se detalla los Estados miembros del Consejo de Europa (47 miembros y 8 observadores). Dentro de los países miembros del consejo europeo, se encuentran los países que han incorporado el Convenio de Budapest sobre la ciberdelincuencia en su legislación nacional para el combate contra los actos ilícitos que involucran las tecnologías de información.

*Estados miembros del Consejo de Europa. Fuente: Council of Europe*

| País | Firma | Ratificación | Entrada en vigor | R. | D. | A. | T. | C. | O. |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Albania | 23/11/2001 | 20/6/2002 | 1/7/2004 |  |  | X |  |  |  |
| Andorra | 23/4/2013 |  |  |  |  |  |  |  |  |
| Armenia | 23/11/2001 | 12/10/2006 | 1/2/2007 |  |  | X |  |  |  |
| Austria | 23/11/2001 | 13/6/2012 | 1/10/2012 | X | X | X |  |  |  |
| Azerbaiyán | 30/6/2008 | 15/3/2010 | 1/7/2010 | X | X | X | X |  |  |
| Bélgica | 23/11/2001 | 20/8/2012 | 1/12/2012 | X | X | X |  |  |  |
| Bosnia y Herzegovina | 9/2/2005 | 19/5/2006 | 1/9/2006 |  |  | X |  |  |  |
| Bulgaria | 23/11/2001 | 7/4/2005 | 1/8/2005 | X | X | X |  |  |  |
| Croacia | 23/11/2001 | 17/10/2002 | 1/7/2004 |  |  | X |  |  |  |
| Chipre | 23/11/2001 | 19/1/2005 | 1/5/2005 |  |  | X |  |  |  |
| República Checa | 9/2/2005 | 22/8/2013 | 1/12/2013 | X | X | X |  |  |  |
| Dinamarca | 22/4/2003 | 21/6/2005 | 1/10/2005 | X |  | X | X |  |  |
| Estonia | 23/11/2001 | 12/5/2003 | 1/7/2004 |  |  | X |  |  |  |
| Finlandia | 23/11/2001 | 24/5/2007 | 1/9/2007 | X | X | X |  |  |  |
| Francia | 23/11/2001 | 10/1/2006 | 1/5/2006 | X | X | X |  |  |  |
| Georgia | 1/4/2008 | 6/6/2012 | 1/10/2012 |  | X |  |  |  |  |
| Alemania | 23/11/2001 | 9/3/2009 | 1/7/2009 | X | X | X |  |  |  |
| Grecia | 23/11/2001 |  |  |  |  |  |  |  |  |
| Hungría | 23/11/2001 | 4/12/2003 | 1/7/2004 | X | X | X |  |  |  |
| Islandia | 30/11/2001 | 29/1/2007 | 1/5/2007 | X |  | X |  |  |  |
| Irlanda | 28/2/2002 |  |  |  |  |  |  |  |  |
| Italia | 23/11/2001 | 5/6/2008 | 1/10/2008 |  |  | X |  |  |  |
| Letonia | 5/5/2004 | 14/2/2007 | 1/6/2007 | X |  | X |  |  |  |
| Liechtenstein | 17/11/2008 |  |  |  |  |  |  |  |  |
| Lituania | 23/6/2003 | 18/3/2004 | 1/7/2004 | X | X | X |  |  |  |
| Luxemburgo | 28/1/2003 |  |  |  |  |  |  |  |  |
| Malta | 17/1/2002 | 12/4/2012 | 1/8/2012 |  | X |  |  |  |  |
| Moldava | 23/11/2001 | 12/5/2009 | 1/9/2009 |  | X | X | X |  |  |
| Mónaco | 2/5/2013 |  |  |  |  |  |  |  |  |

*Estados miembros del Consejo de Europa. Fuente: Council of Europe (Continuación)*

| País | Firma | Ratificación | Entrada en vigor | R. | D. | A. | T. | C. | O. |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Montenegro | 7/4/2005 | 3/3/2010 | 1/7/2010 | X |  | X |  |  |  |
| Países Bajos | 23/11/2001 | 16/11/2006 | 1/3/2007 |  |  | X | X |  |  |
| Noruega | 23/11/2001 | 30/6/2006 | 1/10/2006 | X | X | X |  |  |  |
| Polonia | 23/11/2001 |  |  |  |  |  |  |  |  |
| Portugal | 23/11/2001 | 24/3/2010 | 1/7/2010 |  | X | X |  |  |  |
| Romania | 23/11/2001 | 12/5/2004 | 1/9/2004 |  |  | X |  |  |  |
| Rusia |  |  |  |  |  |  |  |  |  |
| San Marino |  |  |  |  |  |  |  |  |  |
| Serbia | 7/4/2005 | 14/4/2009 | 1/8/2009 |  |  | X |  |  |  |
| Eslovaquia | 4/2/2005 | 8/1/2008 | 1/5/2008 | X | X | X |  |  |  |
| Eslovenia | 24/7/2002 | 8/9/2004 | 1/1/2005 |  |  | X |  |  |  |
| España | 23/11/2001 | 3/6/2010 | 1/10/2010 |  | X | X |  |  |  |
| Suecia | 23/11/2001 |  |  |  |  |  |  |  |  |
| Suiza | 23/11/2001 | 21/9/2011 | 1/1/2012 | X | X | X |  |  |  |
| La ex República Yugoslava de Macedonia | 23/11/2001 | 15/9/2004 | 1/1/2005 |  |  | X |  |  |  |
| Turquía | 10/11/2010 |  |  |  |  |  |  |  |  |
| Ucrania | 23/11/2001 | 10/3/2006 | 1/7/2006 | X |  | X |  |  |  |
| Inglaterra | 23/11/2001 | 25/5/2011 | 1/9/2011 | X |  | X |  |  |  |

En la tabla anterior, se describe como han incorporado el convenio dentro de su legislación vigente. La incorporación puede ser realizada de la siguiente forma:

1. ***R.: Reservas***: Es una declaración unilateral, llevada a cabo al firmar, ratificar, aceptar, aprobar o adherirse al tratado, con el objetivo de excluir o modificar los efectos jurídicos de ciertas disposiciones en su aplicación.
2. ***D.: Declaraciones***: Es un comunicado que aclara el sentido o el alcance en el que se aplicará al convenio por el cual se establece las razones para convertirse en una de las Partes miembros del convenio.
3. ***A.: Autoridades***: Serán los responsables de realizar la difusión y aplicación del convenio en el Estado miembro.
4. ***T.: Aplicación territorial***: Es una declaración realizada para especificar en o los territorios a los que se aplicará el convenio.
5. ***C.: Comunicación***: Es una declaración por la cual se expresan los puntos de vista relacionados con el tratado, se puede notificar la proclamación de una nueva ley, o rectificar un error o una omisión realizada.
6. ***O.: Objeción***: Es una declaración realizada para identificar, puntos con los que se encuentran en desacuerdo o disposiciones a considerar en la aplicación del convenio en el Estado.

**Anexo B. Países no miembros del Consejo Europeo**

En la siguiente tabla se detalla los Estados no miembros del Consejo de Europa. La adhesión al Convenio de Budapest sobre la ciberdelincuencia también se encuentra abierta a países que sean invitados por el Consejo Europeo, para que lo puedan integrar en su legislación nacional.

*Estados no miembros del Consejo de Europa. Fuente: Council of Europe*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| País | Firma | Ratificación | Entrada en  vigor | R. | D. | A. | T. | C. | O. |
| Argentina |  |  |  |  |  |  |  |  |  |
| Australia | 30/11/2012 | 30/11/2012 | 1/3/2013 | X |  | X |  |  |  |
| Canadá | 23/11/2001 |  |  |  |  |  |  |  |  |
| Chile |  |  |  |  |  |  |  |  |  |
| Colombia |  |  |  |  |  |  |  |  |  |
| Costa Rica |  |  |  |  |  |  |  |  |  |
| República  Dominicana | 7/2/2013 | 7/2/2013 | 1/6/2013 |  | X | X |  |  |  |
| Israel |  |  |  |  |  |  |  |  |  |
| Japón | 23/11/2001 | 3/7/2012 | 1/11/2012 | X | X | X |  |  |  |
| Mauricio | 15/11/2013 | 15/11/2013 | 1/3/2014 |  |  | X |  |  |  |
| México |  |  |  |  |  |  |  |  |  |
| Marruecos |  |  |  |  |  |  |  |  |  |
| Panamá | 5/3/2014 | 5/3/2014 | 1/7/2014 |  |  | X |  |  |  |
| Filipinas |  |  |  |  |  |  |  |  |  |
| Senegal |  |  |  |  |  |  |  |  |  |
| Sudáfrica | 23/11/2001 |  |  |  |  |  |  |  |  |
| Estados Unidos | 23/11/2001 | 29/9/2006 | 1/1/2007 | X | X | X |  |  |  |

En la tabla anterior, se describe como han incorporado el convenio dentro de su legislación vigente. La incorporación puede ser realizada de la siguiente forma:

1. ***R.: Reservas:***Es una declaración unilateral, llevada a cabo al firmar, ratificar, aceptar, aprobar o adherirse al tratado, con el objetivo de excluir o modificar los efectos jurídicos de ciertas disposiciones en su aplicación.
2. ***D.: Declaraciones***: Es un comunicado que aclara el sentido o el alcance en el que se aplicará al convenio por el cual se establece las razones para convertirse en una de las Partes miembros del convenio.
3. ***A.: Autoridades***: Serán los responsables de realizar la difusión y aplicación del convenio en el Estado miembro.
4. ***T.: Aplicación territorial***: Es una declaración realizada para especificar en o los territorios a los que se aplicará el convenio.
5. ***C.: Comunicación***: Es una declaración por la cual se expresan los puntos de vista relacionados con el tratado, se puede notificar la proclamación de una nueva ley, o rectificar un error o una omisión realizada.
6. ***O.: Objeción***: Es una declaración realizada para identificar, puntos con los que se encuentran en desacuerdo o disposiciones a considerar en la aplicación del convenio en el Estado.

**Anexo C. Estadísticas de delitos informáticos**

Información sobre los delitos informáticos entregada por la Policía de Investigaciones de Chile (*PDI, como sus siglas lo indican*), mediante consulta realizada por el recurso de la Ley de Transparencia. La PDI, entregó estadísticas de los delitos de sabotaje y espionaje informáticos investigados a nivel nacional como también de las denuncias por las que se obtuvieron detenidos.

*Estadísticas delitos investigados por espionaje informático. Fuente: Policía de Investigaciones de Chile*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Delitos investigados de espionaje informático a nivel nacional | | | | | | | | | | | | | | |
| Año | I | II | III | IV | V | VI | VII | VIII | IX | X | XI | XII | XIV | XV | RM |
| 2015 | 1 | 2 | 0 | 1 | 11 | 1 | 4 | 3 | 8 | 1 | 1 | 3 | 4 | 1 | 69 |
| 2014 | 0 | 3 | 1 | 1 | 6 | 1 | 3 | 8 | 3 | 3 | 2 | 9 | 3 | 0 | 97 |
| 2013 | 1 | 1 | 3 | 2 | 13 | 0 | 9 | 6 | 4 | 4 | 6 | 4 | 1 | 4 | 70 |
| 2012 | 0 | 7 | 1 | 7 | 9 | 5 | 11 | 2 | 4 | 6 | 9 | 10 | 0 | 4 | 74 |
| 2011 | 0 | 9 | 2 | 0 | 12 | 4 | 1 | 4 | 12 | 14 | 20 | 11 | 1 | 4 | 64 |
| 2010 | 0 | 3 | 4 | 2 | 5 | 1 | 2 | 1 | 4 | 7 | 2 | 28 | 0 | 3 | 45 |

*Estadísticas delitos investigados por sabotaje informático. Fuente: Policía de Investigaciones de Chile*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Delitos investigados de sabotaje Informático a nivel nacional | | | | | | | | | | | | | | |
| Año | I | II | III | IV | V | VI | VII | VIII | IX | X | XI | XII | XIV | XV | RM |
| 2015 | 3 | 3 | 2 | 0 | 23 | 3 | 6 | 14 | 7 | 5 | 2 | 2 | 10 | 2 | 328 |
| 2014 | 0 | 1 | 1 | 1 | 19 | 1 | 8 | 12 | 6 | 4 | 3 | 1 | 14 | 0 | 311 |
| 2013 | 0 | 1 | 0 | 0 | 12 | 1 | 4 | 10 | 1 | 15 | 4 | 0 | 0 | 1 | 279 |
| 2012 | 0 | 3 | 1 | 1 | 38 | 4 | 8 | 27 | 5 | 2 | 21 | 0 | 1 | 3 | 341 |
| 2011 | 0 | 136 | 4 | 1 | 13 | 0 | 4 | 33 | 2 | 6 | 12 | 1 | 3 | 1 | 421 |
| 2010 | 0 | 6 | 6 | 3 | 10 | 1 | 2 | 16 | 2 | 11 | 0 | 5 | 0 | 1 | 433 |

**Anexo D. Ley N° 19.223**

Ley N° 19.223 relativa a los delitos informáticos vigente en Chile desde el año 1993.

“*Artículo 1°. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.*

*Si como consecuencia de estas conductas, se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.* (Nacional, 1993)

*Artículo 2°. El que con ánimo de apoderarse, usar, o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.* (Nacional, 1993)

*Artículo 3°. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de la información, será castigado con presidio menor en su grado medio.* (Nacional, 1993)

*Artículo 4°. El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio.*

*Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.* (Nacional, 1993)”

**Anexo E. Artículos del Convenio de Budapest contenidos en la legislación chilena**

Acciones ilícitas tipificadas en el Convenio de Budapest que encuentran contenidos en la Ley 20.526 que sanciona la pornografía infantil y la Ley 17.336 que rige los delitos que atentan contra la propiedad intelectual.

*Artículos del Convenio de Budapest contenidos en la legislación chilena. Fuente: Biblioteca del Congreso Nacional de Chile*

| Artículo | Descripción del artículo |
| --- | --- |
| *Delitos relacionados con la pornografía infantil*  *(Art. 9°)* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito interno la comisión deliberada e ilegítima de los siguientes actos:*    1. *La producción de pornografía infantil con la intensión de difundirla a través de un sistema informático;*    2. *La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;*    3. *La difusión o la transmisión de pornografía infantil a través de un sistema informático;*    4. *La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático.*    5. *La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informático.* 2. *A los efectos del párrafo 1 anterior, se entenderá por “pornografía infantil” todo material pornográfico que contenga la representación visual de:*    1. *Un menor adoptando un comportamiento sexualmente explícito;*    2. *Una persona que parezca un menor adoptando un comportamiento sexualmente explícito;*    3. *Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.* 3. *A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.* 4. *Las Partes podrán reservarse el derecho a un aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.* |

*Artículos del Convenio de Budapest contenidos en la legislación chilena. Fuente: Biblioteca del Congreso Nacional de Chile (Continuación)*

| Artículo | Descripción del artículo |
| --- | --- |
| *Delitos relacionados con infracciones de la propiedad intelectual y de derecho afines*  *(Art. 10°)* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de Julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionándolos con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.* 2. *Cada parta adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.*   *En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales de incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.* |

**Anexo F. Casos de estudio de delitos informáticos chilenos**

Juicios llevados a cabo en Chile, donde se solicitó llevar la causa bajo la ley de delitos informáticos y los jueces por falta de conocimiento y pruebas dictaminaron inadmisibles las causas bajo lo solicitado por los fiscales.

*Descripción caso Hipermercado Curicó limitada con Lizama Ponce. Fuente: Biblioteca Poder Judicial de la República de Chile*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Nombre Caso | Cargos formulados | | Dictamen |
| 1 | *Hipermercado Curicó Limitada con Lizama Ponce, María de las Nieves y otros.* | Cajera de un supermercado se aprovecha del sistema de venta de tarjetas electrónicas de saldo para telefonía móvil para venderlas sin registrar la venta en el sistema interno de cajas.  Se formulan cargos, incluida la comisión del delito contenido en el artículo 1° de la Ley N° 19.223, en tanto se impide, obstaculiza o modifica el funcionamiento de un sistema de tratamiento de información. | | A juicio del tribunal, sólo se aprovecharon de su funcionamiento que estaba mal programado. De esta forma, queda claro que la interceptación debe ser realizada por un medio técnico, elemento ausente en las disposiciones de la Ley N° 19.223. |
| *Rol – Rit*: O – 81 – 2010 | | | *RUC*: 0910014546-1 | *Fecha Ing.*: 09/09/2010 |
| *Caratulado*: Hipermercado Curicó LTDA. C/ Maira de las Nieves Lizama Ponce; María José Rebolledo Muñoz y Carlos Alfredo Rodríguez Guerra | | | | |
| *Materia*: Estafas y otras defraudaciones ART. 468, 467, 469 y 470 (Se excluye el N°1 y N°3) 473. | | | | |
| *Tribunal*: Tribunal de Juicio oral en lo Penal de Curicó | | | | |
| Corte de Apelaciones de Talca, rol 498-2010, resolución del 24 de diciembre de 2010. (Judicial, 2016) | | | | |

*Descripción caso Sky Chile CPA con Merino Moraga, Pablo Andrés. Fuente: Biblioteca Poder Judicial de la República de Chile*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Nombre Caso | Cargos formulados | | Dictamen |
| 2 | *Sky Chile CPA con Merino Moraga, Pablo Andrés.* | Venta de tarjetas de codificación para receptores de señal satelital modificadas para obtener acceso a dichos canales sin pagar a sus operadores.  Se formulan cargos contenidos en la Ley General de Telecomunicaciones, como infracción al artículo 1° de la Ley N° 19.223, al modificar el funcionamiento del sistema de tratamiento de información. | | La Corte Suprema, en un fallo favorable al imputado, establece que el uso de este programa no configura el delito del artículo 1° puesto que no fue creado por él, sino que sólo se trata del uso de un programa obtenido gratuitamente en internet. |
| Libro : Criminal - 4245 - 2008 | | | Estado Recurso: Vigente | Fecha : 28/07/2008 |
| Ubicación: Fallado y devuelto | | | Estado Procesal: Fallada |  |
| Recurso :  CM05 - (Crimen) Casación Fondo | | | | |
| Caratulado: C/ Pablo Merino Moraga. QTE.:SKY Chile S.A | | | | |
| Tribunal: Corte Suprema | | | | |
| Corte Suprema, rol 4245-2008, resolución del 2 de abril de 2009. (Chile P. J., 2012) | | | | |

*Descripción caso Polincay Export y Comercial Polincay Ltda. con Pérez Rodríguez, Raúl Ignacio. Fuente: Biblioteca Poder Judicial de la República de Chile*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N° | Nombre Caso | Cargos formulados | | Dictamen |
| 3 | *Polincay Export y Comercial Polincay Ltda. con Pérez Rodríguez, Raúl Ignacio.* | Obtención de la contraseña de acceso al correo electrónico de su jefe, a fin de acceder al contenido de su computador.  El imputado cometió un abuso de confianza, reenviando otros correos del afectado a cuentas externas para obtener información acerca de su empleador y sus negocios. | | La Corte Suprema, conociendo de una casación en el fondo a la sentencia que absolvía al imputado, se pregunta respecto de la extensión de la palabra indebida en el artículo 2° de la ley. Resuelve que la intromisión no fue indebida, puesto que existió la intromisión de manera autorizada y consentida, estableciendo responsabilidad en la víctima por haber puesto en peligro sus propios datos. |
| Libro : Criminal - 9238 - 2012 | | | Estado Recurso: Vigente | Fecha : 12/12/2012 |
| Ubicación: Fallado y devuelto | | | Estado Procesal: Fallada |  |
| Recurso :  CM05 - (Crimen) Casación Fondo | | | | |
| Caratulado: C/Raúl Ignacio Pérez Rodríguez. QTE.: Rodrigo Fernández Munizaga. | | | | |
| Tribunal: Corte Suprema | | | | |
| Corte Suprema, rol 9238-2012, resolución del 9 de julio de 2013. (Chile P. J., 2012) | | | | |

**Anexo G. Delitos tipificados en el Convenio de Budapest**

Delitos tipificados en el Convenio de Budapest sobre la ciberdelincuencia.

Delitos tipificados en el Budapest sobre la ciberdelincuencia. Fuente: Council of Europe

|  |  |
| --- | --- |
| Artículo | Descripción |
| *2°*  *Acceso Ilícito* | *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno al acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.* |
| *3°*  *Interceptación ilícita* | *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las partes podrán exigir que el delito se cometa con intensión delictiva o en relación con un sistema informático conectado a otro sistema informático.* |
| *4°*  *Ataques a la integridad de los datos* | *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos.*  *Las partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1, comporten daños graves.* |
| *5° Ataques a la integridad de los datos* | *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.* |

Delitos tipificados en el Budapest sobre la ciberdelincuencia. Fuente: Council of Europe (Continuación)

|  |  |
| --- | --- |
| Artículo | Descripción |
| *6°*  *Abuso de los dispositivos* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:* 2. *La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:* 3. *Cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 al 5 del presente Convenio;* 4. *Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y* 5. *La posesión de alguno de los elementos contemplados en los incisos I) y II) del apartado a) del presente artículo con intensión de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.* 6. *No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta obtención para la utilización, importación, difusión o cualquiera otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tengan por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.* 7. *Las partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1.a) II) del presente artículo.* |
| *7°*  *Falsificación informática* | *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos, con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e ilegibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.* |

Delitos tipificados en el Budapest sobre la ciberdelincuencia. Fuente: Council of Europe (Continuación)

|  |  |
| --- | --- |
| Artículo | Descripción |
| *8°*  *Fraude informático* | *Las partes adoptarán las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: La introducción, alteración, borrado o supresión de datos informáticos;*   1. *Cualquiera interferencia en el funcionamiento de un sistema informático, con la intensión, dolosa o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.* |
| *9°*  *Delitos relacionados con la pornografía infantil* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:* 2. *La producción de pornografía infantil con la intensión de difundirla a través de un sistema informático.* 3. *La oferta o puesta a disposición de pornografía infantil a través de un sistema informático;* 4. *La difusión o la transmisión de pornografía infantil a través de un sistema informático;* 5. *La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;* 6. *La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.* 7. *A los efectos del párrafo 1 anterior, se entenderá por “pornografía infantil” todo material pornográfico que contenga la representación visual de:* 8. *Un menor adoptando un comportamiento sexualmente explícito;* 9. *Una persona que parezca un menor adoptando un comportamiento sexualmente explícito ;* 10. *Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.* 11. *A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.* 12. *Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1, y los apartados b) y c) del párrafo 2.* |

Delitos tipificados en el Budapest sobre la ciberdelincuencia. Fuente: Council of Europe (Continuación)

|  |  |
| --- | --- |
| Artículo | Descripción |
| *10°*  *Delitos relacionados con infracciones de la propiedad intelectual y de derecho afines* | 1. *Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en Ia legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de Paris de 24 de julio de 1971 por Ia que se revisó el Convenio de Berna para Ia protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de Ia OMPI sobre Ia propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informática.* 2. *Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en Ia legislación de dicha Parte, de conformidad con las obligaciones que esta haya asumido en aplicación de Ia Convención Internacional sobre Ia protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informática.* 3. *En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo.* |

**Anexo H. Artículos del Convenio de Budapest reservados por Chile**

Chile, en su opción a realizar la adhesión al Convenio de Budapest, ha manifestado que realizará la reserva de cinco artículos, los que se muestran a continuación:

*Artículos del Convenio de Budapest reservados por Chile. Fuente: Biblioteca Congreso Nacional*

|  |  |
| --- | --- |
| Artículo | Descripción del artículo |
| *Ataques a la integridad de los datos*  (Art. 4) | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.* 2. *Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.* |
| *Abuso de los dispositivos (Art. 6)* | *Tipificación de la comisión deliberada e ilegítima de actos:*  *a) De producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos señalados en las celdas anteriores; ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer los delitos señalados en la celdas anteriores.*  *b) La posesión de algunos de los elementos contemplados en i) o ii) del apartado a) con intención de que sean utilizados para cometer cualquiera de los delitos previstos en las celdas anteriores.* |
| *Delitos relacionados con la pornografía infantil*  *(Art. 9)* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:* 2. *La producción de pornografía infantil con la intensión de difundirla a través de un sistema informático.* 3. *La oferta o puesta a disposición de pornografía infantil a través de un sistema informático;* 4. *La difusión o la transmisión de pornografía infantil a través de un sistema informático;* 5. *La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;* 6. *La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.* 7. *A los efectos del párrafo 1 anterior, se entenderá por “pornografía infantil” todo material pornográfico que contenga la representación visual de:* 8. *Un menor adoptando un comportamiento sexualmente explícito;* 9. *Una persona que parezca un menor adoptando un comportamiento sexualmente explícito ;* 10. *Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.* 11. *A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.* |

*Artículos del Convenio de Budapest reservados por Chile. Fuente: Biblioteca Congreso Nacional (Continuación)*

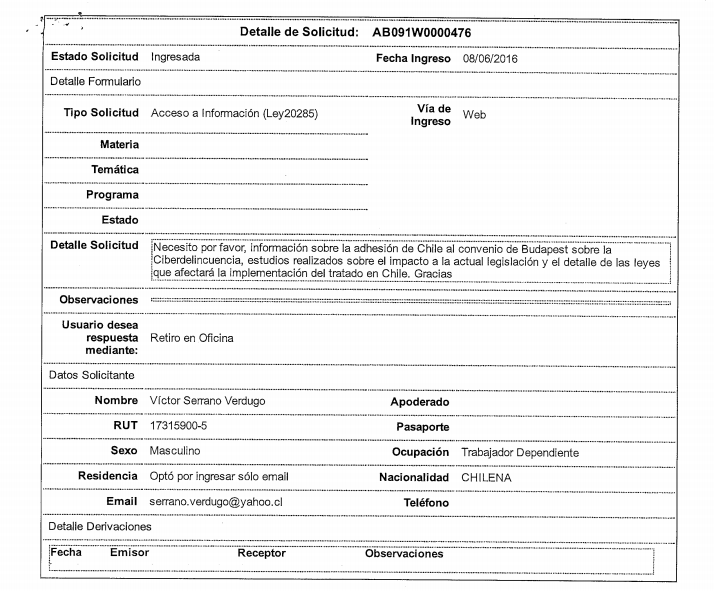
|  |  |
| --- | --- |
| Artículo | Descripción del artículo |
| *Jurisdicción (Art. 22)* | 1. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:* 2. *En su territorio; o* 3. *A bordo de un buque que enarbole su pabellón; o* 4. *A bordo de una aeronave matriculada según sus leyes; o* 5. *Por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.* 6. *Las partes podrán reservarse el derecho a no aplicar, o a aplicar sólo determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.* 7. *Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraído a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.* 8. *En presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.* 9. *En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.* |
| *Conservación rápida de datos informáticos almacenados (Art. 29)* | 1. *Una parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conversación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar solicitud de asistencia mutua con vistas al registro o al acceso por medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.* 2. *En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:* 3. *La autoridad que solicita la conversación* 4. *El delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con los mismos.* 5. *Los datos informáticos almacenados que deban conservarse y su relación con el delito.* 6. *Toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático.* 7. *La necesidad de la medida de conservación* 8. *Que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.* |

*Artículos del Convenio de Budapest reservados por Chile. Fuente: Biblioteca Congreso Nacional (Continuación)*

|  |  |
| --- | --- |
| Artículo | Descripción del artículo |
| *Conservación rápida de datos informáticos almacenados (Art. 29)* | 1. *Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas necesarias adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.* 2. *Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.* 3. *Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:* 4. *La solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político.* 5. *La parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.* 6. *Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.* 7. *Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión.* |

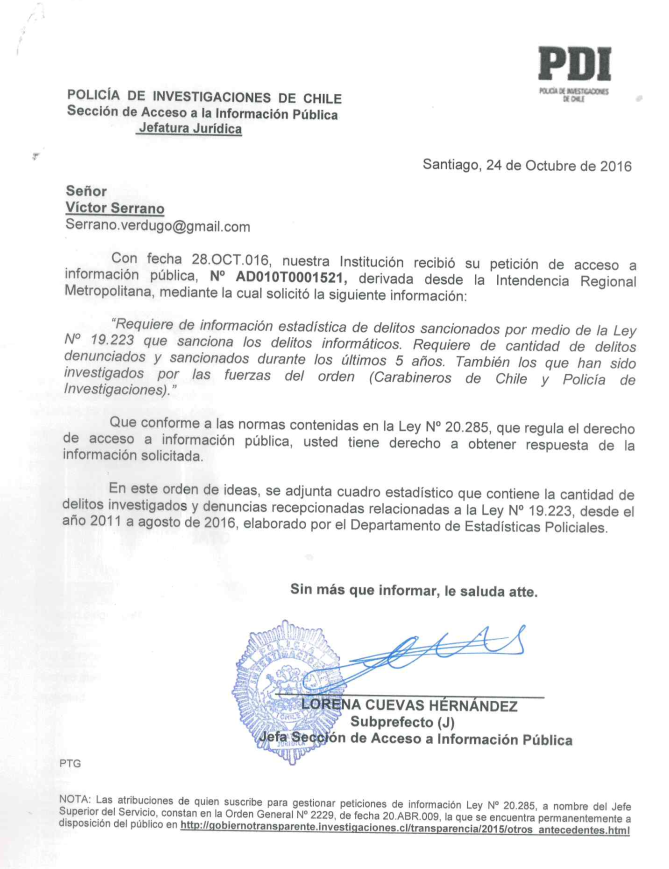
**Anexo I. Solicitudes información Ley de Transparencia**

Solicitud realizada por recurso de Ley de Transparencia para solicitar datos correspondientes a estadísticas de delitos informáticos acontecidos en Chile e información sobre la adhesión de Chile al Convenio de Budapest.



**Anexo J. Respuesta de Policía de Investigaciones de Chile ante solicitud de información por la Ley de Transparencia**

La Policía de Investigaciones de Chile, emitió la siguiente carta en respuesta a la solicitud de datos de delitos informáticos acontecidos en Chile durante el período 2010 – 2015, informando el envío de la información.



**Anexo K. Proyecto de Ley 2974-19**

Modifica la ley Nº 19.223, de 1993, que tipifica figuras penales relativas a la informática.

**Proyecto de Ley**

“*Artículo único.- Modifícase la ley Nº 19.223, de 1993, que tipifica figuras penales relativas a la informática.*

*Sustitúyase el artículo primero de la ley Nº 19.223 por el siguiente:*

*Artículo 1º.- El que sin autorización acceda a un sistema electrónico de almacenamiento o procesamiento de datos, o a través del cual se provee un servicio electrónico de comunicaciones sufrirá la pena de presidio menor en sus grados mínimo a medio, una multa de beneficio fiscal de 50 a 100 Unidades Tributarias Mensuales y una multa del mismo monto a beneficio de cada uno de los afectados, sin perjuicio de las indemnizaciones de daño que se puedan reclamar de conformidad a la ley.*

*Cuando con motivo de dicho acceso se produzca una alteración de los datos almacenados o del funcionamiento del sistema, se aplicará a quien incurra en él, aun sin la intención de causar dicha alteración, la pena de presidio menor en su grado medio y las multas indicadas en el inciso anterior.*

*Sustitúyase el artículo segundo de la ley Nº 19.223 por el siguiente:*

*Artículo 2º.- Cuando el acceso no autorizado descrito en el artículo anterior tenga el propósito de apoderarse de datos, conocerlos indebidamente, obtener ventaja comercial, o se ejecute excediéndose una autorización vigente, se aplicará la pena de presidio menor en sus grados medio a máximo, y las multas respectivas serán de 200 a 500 Unidades Tributarias Mensuales.*

*Sustitúyase el artículo tercero de la ley Nº 19.223 por el siguiente:*

*Artículo 3º.- El que maliciosamente destruya o inutilice un sistema de almacenamiento o procesamiento de datos, obstaculice o modifique su funcionamiento, o modifique o destruya los datos contenidos en él, sufrirá la pena de presidio menor en su grado máximo y las multas indicadas en el artículo anterior*”.

**Anexo L. Proyecto de Ley 7090-07**

Modifica ley N° 19.223, con objeto de establecer sanciones para los funcionarios públicos que, sustraigan datos contenidos en los sistemas de información de sus respectivos servicios.

**Proyecto de Ley**

“*Artículo único: Modificase la Ley N° 19.223, que tipifica las figuras penales relativas a la informática, agregándose el siguiente artículo 5° nuevo:*

*Artículo 5°: Se aplicarán las penas del artículo 1° al funcionario público, cualquiera sea la modalidad de su dependencia de la administración estatal, que antes de ser desvinculado de su respectivo servicio, por cualquier causal contemplada en la ley, sustraiga los datos contenidos en un sistema de información que se encuentre a su cargo.*"

**Anexo M. Proyecto de Ley 9998-07**

Modifica la ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática, sancionando la distribución, exhibición o reproducción de material pornográfico infantil.

**Proyecto de Ley**

“*Incorpora el siguiente artículo 5° a la Ley N°19.223, que tipifica figuras penales relativas a la informática:*

*Artículo 5°: El que procediere a la distribución, exhibición o reproducción por cualquier medio accesible a través de conexiones a internet o telefónicas, material con contenido pornográfico en cuya elaboración o producción hayan sido utilizados o aparecieren menores de edad, aunque el material tuviere su origen en el extranjero o fuere desconocido su origen, sufrirá la pena de presidio menor en su grado máximo. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.*

*Igual pena sufrirá la persona que facilitare las conductas antes descritas, mediante cualquier forma.*

*Lo anterior, sin perjuicio de que la Fiscalía requiera al Juez de Garantía competente la suspensión o clausura, total o definitiva, del dominio, portal o aplicación a través de la cual se procedió a la emisión o difusión del contenido señalado en el inciso primero.*”

**Anexo N. Proyecto de Ley 10145-07**

Tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223.

**Proyecto de Ley**

“*Artículo 1°.- El que maliciosamente destruya o inutilice un sistema informático de tratamiento computacional de datos, o sus partes o componentes lógicos, o limite o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.*

*Si la conducta recayere sobre sistemas de los cuales dependan la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable, alcantarillado, electricidad, transporte, redes domiciliaras de gas o redes cableadas o inalámbricas de telefonía o computación; la pena será de presidio menor en su grado máximo a presidio mayor en su grado mínimo.*

*Artículo 2°.- El que sin derecho acceda o use información contenida en un sistema informático de tratamiento de datos, será castigado con presidio menor en su grado mínimo a medio.*

*Con la misma pena será sancionado el que por vía informática impida a otro acceder a sus datos personales u otros de su propiedad intelectual.*

*Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema informático de tratamiento de datos, será castigado con presidio menor en su grado medio.*

*Si la conducta recayere sobre sistemas de los cuales dependan la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable, alcantarillado, electricidad, transporte, redes domiciliaras de gas o redes cableadas o inalámbricas de telefonía o computación, la pena será de presidio menor en su grado máximo a presidio mayor en su grado mínimo.*

*Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema informático de tratamiento de datos, sufrirá la pena de presidio menor en su grado medio.*

*Si los datos correspondieren a un sistema del cual dependa la defensa nacional, la seguridad pública o la infraestructura crítica del país, como por ejemplo servicios públicos de agua potable, alcantarillado, electricidad, transporte, redes domiciliarias de gas o redes cableadas o inalámbricas de telefonía o computación, la pena será de presidio menor en su grado máximo a presidio mayor en su grado mínimo.*

*Artículo 5°.- La tenencia, posesión, producción, venta, difusión, o cualquier otra forma de puesta a disposición de dispositivos, programas informáticos, aplicaciones, claves, códigos de acceso u otro tipo de elemento informático que permitan o faciliten la comisión de delitos, será sancionada con presidio menor en su grado mínimo a medio.*

*Artículo 6°.- 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 esta ley, y la investigación lo hiciere imprescindible, el tribunal, a petición del Ministerio Público, podrá autorizar la interceptación o grabación de los contenidos de las comunicaciones de esa persona y/o de quienes integraren dicha organización. En lo demás, se estará íntegramente a lo dispuesto en los artículos 222 a 225 del Código Procesal Penal.*

*Bajo los mismos supuestos previstos en el inciso precedente, podrá el tribunal, a petición del Ministerio Público, autorizar la intervención de agentes encubiertos. Del mismo modo el Tribunal podrá autorizar a Carabineros de Chile o la Policía de Investigaciones para 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 se aplicarán también 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 Nº 20.000.*

*Artículo 7°.- El que sin la voluntad de su dueño y con ánimo de lucrar, transfiriere u obtuviere la transferencia de cualquier activo patrimonial de un tercero empleando medios informáticos, será castigado con presidio mayor en sus grados mínimo a medio.*

*Artículo 8°.- Si quien incurriere en las conductas descritas en los artículos anteriores fuere responsable del sistema de información, la pena se aumentará en un grado.*

*Artículo 9°.- Incorpórese la siguiente circunstancia 22ª en el artículo 12 del Código Penal:*

*“22a. Emplear, en cualquiera de sus etapas, medios informáticos para ejecutarlo, entendiéndose por tales cualquier sistema informático de tratamiento de datos de la información.”.*

*Artículo 10°.- Modifíquese el Código Procesal Penal de la siguiente forma:*

*1.- Reemplácese la frase “interceptación de comunicaciones telefónicas” en el encabezado del inciso primero del artículo 222 por “interceptación y registro de comunicaciones”, e Intercálese en ese mismo inciso la frase “los contenidos de” entre las frases “interceptación y grabación de” y “sus comunicaciones telefónicas”.*

*2.- Reemplazase el inciso quinto del artículo 222, por el siguiente:*

*“Toda persona jurídica que, a cualquier título, mantenga o provea acceso a sistemas informáticos de tratamiento de datos, tales como empresas telefónicas, de comunicaciones o de cualquier naturaleza, bancos, establecimientos educacionales, establecimientos comerciales que presten servicios de comunicación digital al público, así como los titulares de redes públicas de conexión inalámbrica, 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. Deberán, además, mantener, en carácter reservado por un lapso no inferior a quince años, a disposición del Ministerio Público, un listado actualizado de los números IP asignados a las conexiones que realicen sus abonados con sus correspondientes fechas y horas, así como de las direcciones físicas asociadas. El encargado de estos registros deberá poner esos datos técnicos a disposición del Ministerio Público, previo requerimiento de información del fiscal a cargo de la investigación, dentro del plazo de veinticuatro horas o del que señale la petición. La negativa o entorpecimiento a la práctica de la medida de interceptación y grabación autorizada judicialmente será constitutivo del delito de desacato, en tanto que el incumplimiento frente al requerimiento de información del Ministerio Público constituirá el delito de obstrucción a la investigación. El fiscal respectivo deberá ejercer las acciones penales que procedan contra el responsable de la negativa, entorpecimiento o incumplimiento tan pronto se haya cumplido el plazo dentro del cual la empresa haya debido cumplir con la obligación que se establece en este inciso. El fiscal que incumpliere esta obligación dentro del plazo prescrito en el artículo 176, incurrirá en el delito previsto y sancionado en el artículo 177. 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”.*

*Artículo 11.- La tentativa y la frustración de los delitos contemplados en esta ley, serán sancionados de acuerdo con las reglas generales contenidas en el Párrafo 4°, del Título III del Libro Primero del Código Penal.*

*Artículo 12.- Deróguese la ley N° 19.223.”*