



PROYECTO DE LEY DE DELITOS INFORMÁTICOS¹

1. ANTECEDENTES

En mayo de 1993 se promulgó la Ley N° 19.223, que “Tipifica figuras penales relativas a la informática”. En sus cuatro artículos, la ley estableció los tipos penales de “sabotaje informático” (daño de los sistemas de tratamiento de información) y “espionaje informático” (acceso con ánimo de apropiación, uso o conocimiento a información contenida en redes informáticas), además de sancionar el daño y divulgación de datos contenidos en un sistema de información². A pesar de que la ley quedó rápidamente superada por el desarrollo de las tecnologías digitales, los intentos por reformarla fueron infructuosos, con lo que muchas conductas delictuales cometidas a través de Internet (cibercrímenes) carecen hasta la fecha de una tipificación específica.

El 23 de noviembre de 2001 se suscribió en Budapest (Hungría) el Convenio sobre la Ciberdelincuencia del Consejo de Europa, también conocido como “Convenio de Budapest”, que tiene como objetivo armonizar las disposiciones en materia de delitos informáticos³. El Convenio de Budapest define los delitos de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos de pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual⁴.

Chile es uno de los países no europeos que ha adherido al Convenio de Budapest –en vigor desde 2004– como parte de su Política Nacional de Ciberseguridad 2017-2022. El Convenio de Budapest fue aprobado por el Congreso Nacional en noviembre de 2016, siendo promulgado en la legislación chilena mediante el Decreto 83 del 27 de abril de 2017, y entró en vigencia el 28 de agosto del mismo año⁵.

2. CONTENIDO

El 25 de octubre de 2018, el Presidente de la República envió al Congreso Nacional el proyecto de ley de delitos informáticos, bajo el Mensaje N° 164-366. Este proyecto deroga la Ley N° 19.223, y establece normas sobre delitos informáticos, siguiendo los tipos definidos por el Convenio de Budapest. Los ciberdelitos que propone el proyecto de ley son:

1. Perturbación informática: Obstaculización o perturbación maliciosa del funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos (pena: presidio menor en su grado medio a máximo). Agravante: Hacer imposible la recuperación del sistema informático en todo o en parte (pena: presidio menor en su grado máximo).

2. Acceso ilícito: Acceso indebido a un sistema informático (pena: presidio menor en su grado mínimo o multa de 11-20 UTM). Agravantes: Acceso indebido con el ánimo de apoderarse, usar o conocer la información contenida en un sistema informático (presidio menor en su grado mínimo a medio); vulneración, evasión o transgresión de medidas de seguridad destinadas para impedir dicho acceso (pena: presidio menor en su grado medio).

3. Interceptación ilícita: Interceptación o interferencia indebida y maliciosa de la transmisión no pública de información entre los sistemas informáticos (pena: presidio menor en su grado mínimo a medio). Agravante: Captación ilícita de datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas de los dispositivos (pena: presidio menor en su grado medio a máximo).

¹ Boletín N° 12192-25. https://www.camara.cl/pley/pley_detalle.aspx?prmID=12715&prmBoletin=12192-25

² <https://www.leychile.cl/Navegar?idNorma=30590>

³ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c>

⁴ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa403>

⁵ <https://www.leychile.cl/Navegar?idNorma=1106936>



4. Daño informático: Alteración, borrado o destrucción maliciosa de datos informáticos, siempre que ello cause un daño serio al titular de los mismos (pena: presidio menor en su grado medio).

5. Falsificación informática: Introducción, alteración, borrado, deterioro, daño, destrucción o supresión maliciosa de datos informáticos con la intención de que sean tomados o utilizados a efectos legales como auténticos (penas: artículo 197 del Código Penal). Atenuante: Los datos sean o formen parte de un instrumento, documento o sistema informático de carácter público (penas: artículo 193 del Código Penal).

6. Fraude informático: Uso de la información contenida en un sistema informático o aprovechamiento de la alteración, daño o supresión de documentos electrónicos o de datos transmitidos o contenidos en un sistema informático, que causa perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero (pena: presidio menor en sus grados medio a máximo y multas de 11-30 UTM, dependiendo del perjuicio).

7. Abuso de los dispositivos: Entrega u obtención para su utilización, importación, difusión o realización de otra forma de puesta a disposición de uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de los delitos de uso fraudulento de tarjeta de crédito o débito (Ley N° 20.009) y de los delitos de perturbación informática, acceso ilícito, interceptación ilícita y daño informático, para la perpetración de dichos delitos (pena: presidio menor en su grado mínimo y multa de 5-10 UTM).

El proyecto de ley también incorpora procedimientos especiales para la investigación de estos delitos, y modifica el Código Procesal Penal, incorporando la obligación de las empresas de telecomunicaciones que presten servicios a los proveedores de acceso a Internet y también a estos últimos, de preservar provisoriamente los datos informáticos por un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días.

Finalmente, el proyecto modifica la Ley N° 20.393⁶, sumando los delitos informáticos a aquellos que generan la responsabilidad penal de las personas jurídicas (lavado de activos, financiamiento del terrorismo, receptación y delitos de cohecho).

Para más información contactar al socio **Edmundo Varas** (evaras@moralesybesa.cl) o al asociado **Marco Correa** (mcorrea@moralesybesa.cl), del área de **Propiedad Intelectual y Protección de Datos**, o al socio **Gonzalo Cordero** (gcordero@moralesybesa.cl) o a la asociada **Rebeca Zamora** (rzamora@moralesybesa), del área de **Derecho Penal y Compliance**.

* * *

Morales & Besa

⁶ Su última modificación se realizó por la Ley N° 21.121, que incorporó nuevos delitos, la cual se publicó en el Diario Oficial el día 20 de noviembre del presente año.

La información contenida en este Informativo no constituye ni pretende constituir asesoría o asistencia legal directa o indirecta de especie alguna. En consecuencia, el lector no debe considerar la información contenida en este documento como asesoría legal de tipo alguno. Además, la información contenida en este Informativo no constituye un requerimiento de parte de nuestra firma ni de alguno de sus abogados para el establecimiento de una relación profesional de cualquier especie. Finalmente, la información contenida en este Informativo no pretende hacer publicidad de los servicios prestados por nuestra firma ni por alguno de sus abogados. El único objetivo del presente Informativo es dar información de carácter general respecto de materias que, en atención a su continua evolución, pueden ser de interés para nuestros clientes.