GUTIÉRREZ & ARRIETA
DERECHO - REGULACIÓN - TECNOLOGÍA

PROYECTO DE LEY DE DELITOS INFORMÁTICOS

Boletín 12.192-25.

El año 2004 entró en vigor el Convenio de Budapest. Su principal objetivo es el desarrollo de una política criminal común frente a la ciberdelincuencia, mediante la homologación de conceptos y tratamiento de la legislación penal dentro del Consejo de Europa

Este Convenio, si bien fue diseñado para su implementación dentro del Consejo de Europa, cabe advertir que algunos Estados no miembros de dicho consejo fueron invitados a hacerse parte, entre ellos Chile, que promulgó el Convenio en abril del 2017 por medio del Decreto Nº 83 del Ministerio de Relaciones Exteriores entrando en vigor en agosto de ese año.

Con ocasión de la promulgación por parte de Chile al Convenio de Budapest, considerando, además, el actual desarrollo tecnológico, el cual ha implicado el surgimiento de nuevos riesgos y ataques contra bienes jurídicos que no se encuentran protegidos por la actual normativa, la Ley 19.223 que tipifica los delitos informáticos, la cual, cabe advertir, no ha sido modificada desde su dictación en 1993, ha ingresado al Congreso un Proyecto de Ley que deroga la normativa vigente y modifica otros cuerpos legales con el objeto de adecuar su regulación al Convenio de Budapest.

El Proyecto de Ley inicia su tramitación por el Senado y, entre las principales modificaciones propuestas, se encuentran:

1. Modificaciones a tipos penales de la Ley 19.223.

Se adecuan los tipos penales ya contenidos en la ley 19.223: sabotaje y espionaje informático, a las figuras reconocidas en el Convenio de Budapest: acceso ilícito a todo o parte de un sistema informático, ataque a la integridad del sistema y de los datos informáticos.

2. Incorporación de nuevos delitos.

El Proyecto de Ley incorpora, entre los artículos 1 y 7, nuevos delitos informáticos en concordancia con el Convenio de Budapest:

a. **Perturbación Informática:**
   La obstaculización o perturbación en el funcionamiento de un sistema informático a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos.

b. Acceso Ilícito:

Acceso indebido a un sistema informático. Si es con ánimo de apoderamiento, uso o conocimiento de información contenida en un sistema informático su pena será aún mayor, así como también si en la comisión de dichas conductas se vulnerasen, evadiesen o transgrediesen medidas de seguridad destinadas a impedir ese acceso.

c. Interceptación ilícita:

Interceptación o interferencia indebida y maliciosa de la transmisión no pública de información entre sistemas informáticos. Aumentará la pena en un grado si se captare la información por medio de sistemas informáticos a través de emisiones electromagnéticas de los dispositivos.

d. Daño informático:

Alterar, borrar o destruir datos informáticos, siempre que con ello cause un daño serio al titular de ellos.

e. Falsificación Informática:

Introducción, alteración, borrado, deterioro, daño, destrucción o supresión maliciosa de datos informáticos con la intención de hacerlos pasar como "auténticos" o "fiables" por un tercero.

f. Fraude informático:

Causar perjuicio a otro y con la finalidad de obtener un beneficio económico ilícito para sí o para un tercero, por medio de la utilización de información contenida en un sistema informático o aprovechamiento de la alteración, daño o supresión de documentos electrónicos o datos transmitidos o contenidos en un sistema informático.

La pena en este caso irá asociada al monto del beneficio económico obtenido.

g. Abuso de dispositivos:

Sanciona a quien, entregue u obtenga para su utilización, importe, difunda o disponibilice de otra forma 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 siguientes delitos:

i. Perturbación Informática,
ii. Acceso Ilícito,
iii. Interceptación Ilícita,
iv. Daño Informático o
v. uso fraudulento de tarjeta de pago.

3. Incorporación de circunstancias atenuantes y agravantes.

El Proyecto de Ley contempla circunstancias modificatorias de responsabilidad, entre las cuales destacan:

a. Atenuantes:

   Se considera como situación atenuante la colaboración relevante que permita:

   i. El esclarecimiento de los hechos
   ii. identificación de los responsables
   iii. prevenir o impedir la perpetración o consumación de otros delitos.

b. Agravantes:

   Entre las situaciones agravantes se considera:

   i. Uso de encriptación con la finalidad de inutilizar u obstaculizar la acción de la justicia.
   ii. Comisión de delito abusando de una posición privilegiada de garante o custodio de datos.
   iii. Afectación o alteración a la provisión o prestación de servicios considerados como de utilidad pública por perturbación al sistema informático o ataque a los datos informáticos.

4. Modificaciones a las reglas de procedimiento

Junto con incorporar nuevos tipos penales, el Proyecto de Ley incorpora, en su título II, reglas especiales de tipo procedimental. Al respecto, dentro de las principales modificaciones están, sin perjuicio de las reglas generales contenidas en el Código Procesal Penal:

a. El reconocimiento de la legitimidad activa al Ministerio del Interior y Seguridad Pública, delegados presidenciales regionales y provinciales.
b. Autorización para usar técnicas especiales de investigación cuando existan sospechas fundadas de la participación de asociaciones ilícitas o agrupaciones delictivas.