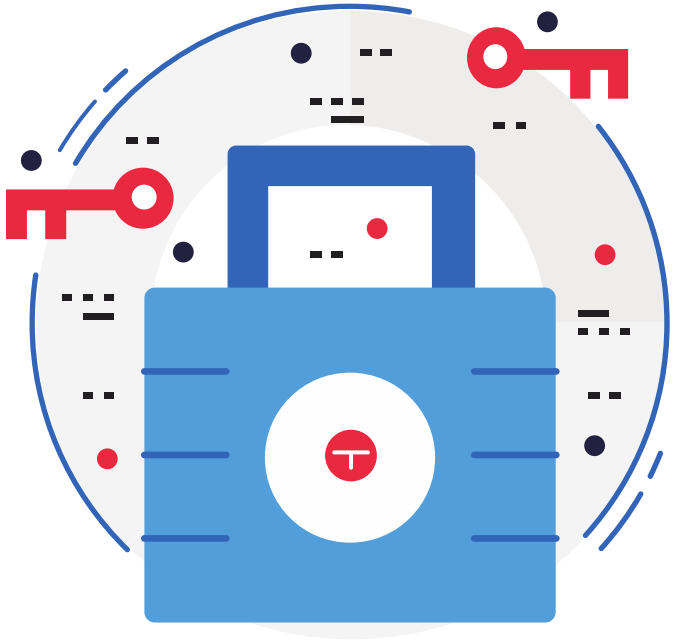
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

Proyecto de Ley Delitos Informáticos



Ministerio de Interior y Seguridad Publica

Nov. 2018

ACTUAL NORMATIVA EN MATERIA DE DELITOS INFORMÁTICOS

La Ley Nº 19.223, sobre **Delitos Informáticos** fue dictada en 1993. En dicha época, la penetración de Internet en Chile era reducida.

La ley protege (bien jurídico) el sistema de tratamiento de información, es decir, hardware (servidores) y no softwares (programas computacionales).

Ello ha provocado que la Ley Nº 19.223 sea insuficiente para responder adecuadamente al fenómeno delictivo informático.

ACTUAL NORMATIVA EN MATERIA DE DELITOS INFORMÁTICOS (Cont)

Los tipos penales que contiene son.

Sabotaje Informático (artículo 1 y 3)	Destrucción o inutilización de un sistema de tratamiento de información. Alteración, daño o destrucción de datos contenidos en un sistema de tratamiento de información.	Presidio Menor en su grado medio a máximo (3 años y 1 día a 5 años). Presidio menor en su grado menor a su grado medio (541 días a 3 años).
Espionaje Informático (artículo 2)	Apoderarse, usar o conocer indebidamente información contenida en un sistema de información, interceptándolo, interfiriendo o accediendo a él.	Presidio menor en su grado mínimo a medio. (541 días a 3 años).
Revelación Informática (artículo 4)	Revelación o difundir datos contenidos en un sistema de información.	Presidio menor en su grado medio (541 días a 3 años). Si el que lo realice es el responsable del sistema de tratamiento, se aumenta un grado.

CONTEXTO ACTUAL

- El **cibercrimen** tiene varios componentes de compleja persecución penal como su naturaleza transnacional e inmediatez en la afectación de varios bienes jurídicos.
- De acuerdo al **Informe presentado por PDI** en abril del 2018, los delitos informáticos habrían aumentado un **74% en el año 2017**, en relación al año 2016. Entre los delitos más comunes se encuentra el Phising, Pharming, etc.
- Nuestra normativa no tiene ninguna norma procesal, lo que impide una adecuada investigación a los entes de persecución, debiendo recurrir a las técnicas generales contenidas en el Código Procesal Penal.

CONTEXTO ACTUAL (cont.)

Durante el 2017, se dictó una **Política Nacional de Ciberseguridad** (2017-2022) que entre sus medidas se encuentra *"la actualización de nuestra legislación en materia de delitos informáticos".*

El mismo año, Chile se adhirió al Convenio sobre Ciberdelincuencia del Consejo de Europa (**Convenio de Budapest**), instrumento internacional sobre esta materia y que fija estándares al respecto.

PROYECTO DE LEY

Es una esfuerzo legislativo para actualizar nuestra normativa en materia de Delitos Informáticos, además, de cumplimiento de obligaciones internacionales.

- Deroga la Ley Nº 19.223, aunque adecua algunos tipos penales a los descritos en el Convenio de Budapest.
- Incorpora nuevos delitos informáticos, tales como: *falsificación informática, fraude informático y abuso de dispositivo.*
- Incluye mejoras sustantivas y procesales.
- Realiza modificaciones en otros cuerpos normativos (Código Procesal Penal y Ley Nº 20.393, sobre Responsabilidad Penal de las Personas Jurídicas).

ASPECTOS GENERALES DEL PROYECTO

DEFINICIONES

- Datos Informáticos.
- Sistema Informático.
- Datos relativos al tráfico.

ADECUACIONES A TIPOS PENALES EXISTENTES

- Perturbación informática.
- Acceso Ilícito.
- Interceptación ilícita.
- Daño informático.

NUEVOS TIPOS PENALES

- Falsificación Informática.
- Fraude informático.
- Abuso de dispositivo.

MEJORAS SUSTANTIVAS.

- Atenuantes especiales.
- Agravantes específicas.

MEJORAS PROCESALES

- Posibilidad de presentar querella al Ministerio del Interior y Seguridad Pública, en ciertos supuestos.
- Técnicas especiales de investigación en este tipo de delitos.
- Instrucciones generales del Fiscal Nacional en materia de evidencia electrónica.

MODIFICACIONES AL CÓDIGO PROCESAL PENAL

- Se agrega una norma sobre “preservación provisoria de datos”.
- Se modifica el artículo 219 del Código Procesal Penal, sobre entrega de copia de las comunicaciones.
- Se incluyen definiciones y especificaciones en el artículo 222 del Código Procesal Penal, sobre interceptación de las comunicaciones.

MODIFICACIÓN LEY DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURIDICAS

- Se agregan los delitos informáticos como supuesto en que las personas jurídicas puedan responder penalmente.

DEFINICIONES

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

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

Datos relativos al tráfico: los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, la localización del punto de acceso a la red, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

ADECUACIONES TIPOS PENALES

Tipo penal Proyecto Ley	Penalidad	Tipos de la Ley Nº 19.223.
Perturbación Informática: sanciona al que obstaculice o perturbe el funcionamiento de un sistema informático.	541 días a 5 años (Presidio menor en su grado medio a máximo). Si no es posible recuperar la información del sistema informático, la pena es de 3 años y 1 día a 5 años (presidio menor en su grado máximo).	Artículo 1, sobre Sabotaje al sistema de tratamiento de información.
Acceso Ilícito: sanciona al que acceda indebidamente a todo o parte de un sistema informático.	61 días a 540 días o multa de 11 a 20 UTM. Si se apodera, usa o conoce la información: 61 días a 3 años (presidio menor en grado mínimo a medio). Si hay vulneración, evasión o transgresión de medidas de seguridad: 541 días a 3 años (presidio menor en grado medio).	Artículo 2, Espionaje Informático.
Interceptación o interferencia a las transmisiones no públicas entre sistemas informáticos.	61 días a 3 años (presidio menor en su grado medio); Si se captan ilícitamente los datos de transmisiones electromagnéticas, 541 días a 5 años (presidio menor en su grado medio a máximo).	Puede estar contenido en el artículo 1º y 2º, cuando se usan los versos “impida, obstaculice o modifique” o “interceptándolo, interfiriéndolo o accediendo”. Con todo, tiene una naturaleza diversa.
Daño Informático: alteración, borrado o destrucción de datos informáticos causando un daño serio al titular.	541 a 3 años (presidio menor en su grado medio).	Artículo 3º, daño informático.

NUEVOS TIPOS PENALES

DELITO DE FALSIFICACIÓN INFORMÁTICA

Comprende la introducción maliciosa, alteración, borrado, deterioro, daño, destrucción o supresión que genere datos no auténticos con el propósito que sean tomados o utilizados como "*auténticos*".

Pena: Esto será sancionado con las penas de presidio menor en cualquiera de sus grados, prevista en el Código Penal, salvo que sean o formen parte de un instrumento, documento o sistema informático de carácter público, caso en que se sancionará con los agravantes previstas en el artículo 193 del citado cuerpo legal.

Ejemplo: Alterar datos de otros, para hacerse pasar por un tercero.

DELITO DE FRAUDE INFORMÁTICO.

Sanciona a quien defraude a otro y con la finalidad de obtener un beneficio económico ilícito para sí o un tercero, utilizando la información contenida en un sistema informático o aprovechándose de la alteración, daño o supresión de documentos electrónicos:

Pena:

- Si el valor del perjuicio excediere de **400 UTM**, con presidio menor en su grado máximo (3 años y 1 días a 5 años) y multa de 21 a 30 UTM.
- Si el valor del perjuicio excede de **40 UTM**, con presidio menor en sus grados medio a máximo (541 días a 5 años) y multa de 11 a 15 UTM.
- Si el valor del perjuicio fuese entre **4 - 40 UTM**, con presidio menor en su grado medio (541 días a 3 años) y multa de 6 a 10 UTM.
- Si el valor del perjuicio no excediere de **4 UTM**, con presidio menor en su grado mínimo (61 días a 540 días) o multa de 5 a 10 UTM.

Ejemplo: Robo al Banco Chile a través de fraude informático al software SWIFT.

ABUSO DE LOS DISPOSITIVOS

Sanciona a quienes entregaren u obtuvieren para su utilización, importaren, difundan o realicen otra forma de puesta a disposición de uno o más dispositivos o programas computacionales u otros datos similares, **creados o adaptados principalmente** para la **perpretación de los delitos** de pertubación al sistema informático, acceso ilícito, interceptación ilícita y daño a los datos informáticos, o aquellos contenidos en el artículo 5º de la Ley sobre Extravío, Robo o Hurto de Tarjetas de Crédito o Débito.

Pena: será de presidio menor en su grado mínimo (61 días a 540 días) y multa de 5 a 10 UTM.

Ejemplo: mecanismos para clonar tarjetas de crédito, copiar bandas magnéticas o de sistemas de acceso restringido, los llamados “skimming”.

NUEVAS MEJORAS SUSTANCIALES

ATENUANTES Y AGRAVANTES

ATENUANTE ESPECIAL

- Permite rebajar hasta un grado, cuando se acredite la cooperación eficaz que conduzca al esclarecimiento de hechos investigados o permita identificar a los responsables o, impedir la perpetración o consumación de estos delitos, entre otros supuestos.

AGRAVANTES

- Utilizar tecnologías de encriptación sobre datos informáticos contenidos en sistemas informáticos que tengan por **principal finalidad** la obstaculización de la acción de la justicia.
- Cometer el delito abusando de una posición privilegiada de garante o custodia de los datos informáticos contenidos en un sistema informático, en razón del ejercicio de un cargo o función.
- Si como resultado de los delitos de perturbación informática o daño a los datos informáticos, se altere o interrumpiese la provisión o prestación de servicios de utilidad pública.

NUEVAS MEJORAS PROCESALES

PROCEDIMIENTO

LEGITIMACIÓN ACTIVA.

- El Ministro del Interior y Seguridad Pública, los delegados presidenciales regionales y delegados presidenciales provinciales pueden presentar querella cuando los delitos informáticos interrumpan el normal funcionamiento de un servicio de utilidad pública.

TÉCNICAS ESPECIALES DE INVESTIGACIÓN.

- En aquellas investigaciones que lo hiciese imprescindible y existieren fundadas sospechas, basadas en determinados de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, se pueden usar las técnicas descritas en los artículos 222 al 226 del Código Procesal Penal y además, los artículos 23 y 25 de la Ley Nº 20.000 (agente encubiertos e informantes).

EVIDENCIA ELECTRÓNICA

COMISO

- Se establece una regla especial de comiso de los efectos y de las utilidades que se hubieren originado con ocasión de la realización de los delitos informáticos, cualquier sea la naturaleza jurídica.

INSTRUCCIONES GENERALES

- Aquellos antecedentes de investigación que se encuentren en formato electrónico serán tratados en conformidad a los estándares definidos para su preservación o custodia, de acuerdo a las instrucciones del Fiscal Nacional.

MODIFICACIONES AL CÓDIGO PROCESAL PENAL

MODIFICACIÓN EN TÉCNICAS DE INVESTIGACIÓN

PRESERVACIÓN PROVISORIA.

- Se agrega un nuevo artículo (218 bis Código Procesal Penal) que permite requerir la preservación de datos informáticos o informaciones concretas incluidas en sistemas informáticos que se encuentren en disposición de los proveedores de acceso a Internet hasta la obtención de autorización judicial.

COPIAS DE LAS COMUNICACIONES.

- Se reemplaza completamente el artículo 219 del Código Procesal Penal, fijando requisitos, condiciones de entrega y responsabilidades frente a la entrega (o negativa) de datos o informaciones acerca de las comunicaciones transmitidas o recibidas por las empresas concesionarias de servicio público de telecomunicaciones que preste servicios a los proveedores de acceso a Internet y también a estos últimos, siempre y cuando exista autorización judicial.

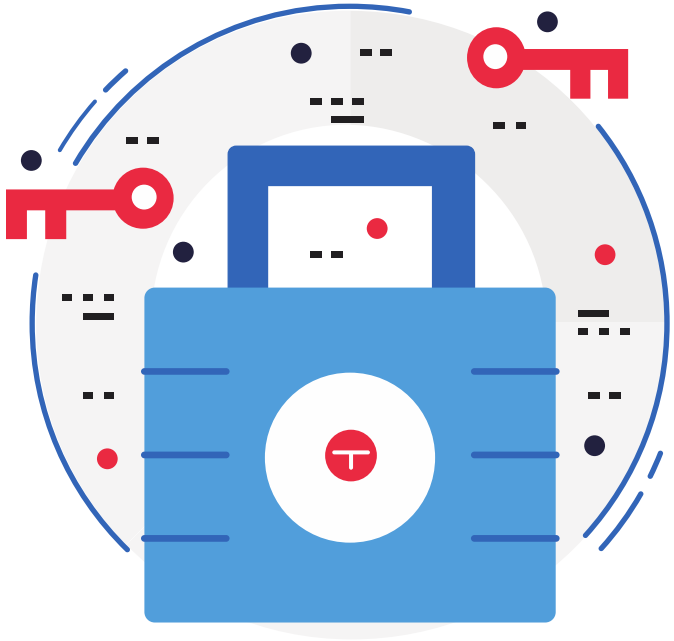
MODIFICACIÓN EN TÉCNICAS DE INVESTIGACIÓN

INTERVENCIÓN DE LAS COMUNICACIONES Y CONSERVACIÓN DE LOS DATOS RELATIVOS AL TRÁFICO.

- Se aumenta el plazo de retención de datos (listado y registro actualizado del rango autorizado de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, datos relativos al tráfico y los domicilios o residencias de sus clientes o usuarios) a **dos años**. En caso de incumplimiento de esta obligación por parte de las empresas de telecomunicaciones, se sancionará en conformidad a la Ley General de Telecomunicaciones.
- Se agrega una definición de datos relativos al tráfico.
- Se establece la obligación de secreto por los empleados quiernes tienen realizan las diligencias decretadas.

Gobierno de Chile

MUCHAS GRACIAS



Convenio Budapest

- Dictado en el 2001 por el Consejo de Europa. Primera armonización entre los estados partes de delitos informáticos realizados por vías telemáticas. Chile lo suscribió el 27 de abril del (Decreto 83 del Min. RREE)
- Los delitos que describe el Convenio de Budapest son:

  Delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Acceso Ilícito , Interceptación ilícita, Ataques a la integridad de los datos. Ataques a la integridad del sistema,

  Abuso de los dispositivos . Falsificación informática. Fraude informático

  Delitos relacionados con infracciones de la propiedad intelectual y los derechos afines.

  Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines .

PROYECTO DE LEY

- Por ende, en términos generales, nuestra Ley sobre delito informático (Nº 19.223) y teniendo en cuenta los comentarios antes indicados de los problemas que se presentan, contempla gran parte de los delitos descritos en el Convenio de Budapest debiendo tipificarse los relativos al **abuso de dispositivos** (art. 6), **falsificación informática** (art. 7) y **fraude informático** (art.8).
- Se resalta lo relativo a la responsabilidad de las personas jurídicas (art. 12 del Convenio de Budapest) y que implica una modificación en la Ley Nº 20.293 sobre Responsabilidad Penal de las Personas Jurídicas.