4.- Ley Nro. 19.233 sobre delitos informáticos

DELITOS INFORMATICOS

LEY CHILENA DE DELITOS INFORMÁTICOS

LEY 19.233 QUE TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA O "LEY DE DELITOS INFORMÁTICOS".

Identificación de la Norma: **Ley-19.223**
Fecha de publicación: **07.06.1993**
Fecha de Promulgación: **28.05.1993**

1. ¿Qué es lo que se protege en la Ley de Delitos Informáticos?
2. ¿Qué es un Delito Informático?
3. ¿Cuáles son las conductas sancionadas en la Ley?
4. ¿En qué consiste el Sabotaje Informático?
5. ¿En qué consiste el Espionaje Informático?
6. ¿Cuáles son las penas de estos delitos?
7. ¿Quiénes pueden querellarse contra estas conductas?

El presente artículo intentará presentar de la forma más simple y completa posible, las conductas que la ley sanciona como, con el objeto es que tomen conocimiento del contenido de la ley y reglamentos y se prevengan y abstengan de incurrir en dichas acciones.

Ley 19.233 “LEY DE DELITOS INFORMATICOS”. TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA.

1. ¿Qué es lo que se protege en la Ley de Delitos Informáticos?

Toda tipificación de delitos pretende, en último término, proteger bienes jurídicos.

Los bienes jurídicos son intereses relevantes de las personas en tanto sujetos sociales, considerados especialmente valiosos y consecuentemente, dignos de protección penal frente a conductas que los dañan o ponen en peligro.

Así, respecto del delito de hurto, por ejemplo, el bien jurídico protegido es la propiedad. En el caso del homicidio, el bien jurídico protegido es la vida.

En el caso de los delitos tipificados en la Ley 19.233, es “un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, la pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan”.

Sin embargo, no sólo se protege ese bien sino que además, concurren otros, tales como: el patrimonio, en el caso de los fraudes informáticos; la privacidad, intimidad y confidencialidad de los datos como es el caso del espionaje informático; la seguridad y fiabilidad del tráfico jurídico y probatorio en el caso de las falsificaciones de datos probatorios vía medios informáticos; el derecho de propiedad sobre la información y sobre los elementos físicos, materiales de un sistema informático, en el caso de los delitos de daños.

2. ¿Qué es un Delito Informático?

Se ha conceptualizado el delito informático de distinta manera, entre las cuales podemos señalar:

a.- “Aquellos delitos perpetrados por medio del uso de computadores y todos los delitos en que se dañe a los computadores o a sus componentes”;

b.- “Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores
jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actué con o sin ánimo de lucro” (Marcel Huerta y Claudio Líbano).

Lo esencial radica en que, tanto los medios de comisión como el objeto del delito, dicen relación con dispositivos habitualmente utilizados en actividades informáticas.

3. ¿Cuáles son las conductas sancionadas en la Ley?

La Ley No 19.223 contempla cuatro artículos, que si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas:

I) Sabotaje Informático.
II) Espionaje Informático.

Estas dos figuras se subdividen en categorías distintas, atendiendo al objeto contra el cual se atenta y/o al modus operandi.

A continuación se transcriben las disposiciones 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".

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".

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".

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".

4. ¿En que consiste el Sabotaje Informático?

El Sabotaje Informático (artículos 1 y 3 de la Ley No 19.223) comprende aquellas conductas tipificadas atendiendo al objeto que se afecta o atenta con la acción delictual, y que puede ser un sistema de tratamiento de la información o de sus partes componentes, el funcionamiento de un sistema de tratamiento de la información, y/o los datos contenidos en un sistema automatizado de tratamiento de la información. El atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación.

5. ¿En que consiste el Espionaje Informático?

El Espionaje Informático (artículo 2 y 4 de la Ley No 19.223) comprende aquellas figuras delictivas que atienden al modo operativo que se ejecuta y que pueden ser, en primer lugar, delitos de apoderamiento indebido (apropiarse de la información), uso indebido (usar la información para cualquier fin) o conocimiento indebido de la información, cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos. Estas figuras se encuentran descritas en el artículo 2o de la Ley, y comprende lo comúnmente conocido como “hacking”. En segundo lugar, comprende también los delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información (artículo 4o de la ley).

6. ¿Cuáles son las penas de estos delitos?

Las penas asignadas a los delitos son bastantes altas.

a) Para el caso de Figuras de Sabotaje Informático:
En el caso de las figuras del Artículo 1o, a las conductas de destrucción e inutilización de un sistema de tratamiento de información o de sus partes o componentes, y a las conductas de impedimento, obstaculización o modificación de su funcionamiento, las penas asignadas van desde 541 días a 5 años. Para el caso que dichas conductas traigan como consecuencia la destrucción de los datos, la pena asignada va de 3 años y un día a 5 años. En el caso del Artículo 3o, las conductas de destrucción, daño o alteración maliciosa de los datos, tienen asignadas penas que van desde los 541 días a los 3 años.

b) Para el caso de Figuras de Espionaje Informático:
En el caso del Artículo 2o, esto es, las conductas de apoderamiento, uso y conocimiento indebido mediante la interceptación, interferencia y acceso al sistema, las penas van desde 61 días a 3 años. Finalmente, en lo que respecta al Artículo 4o, las conductas de revelación o difusión maliciosa de los datos, tienen penas que van desde los 541 días hasta 3 años. Si la persona que incurre en estas conductas es el encargado del sistema, la pena sube de 3 años y un día a 5 años.

7. ¿Quiénes pueden querellarse contra estas conductas?

No hay limitaciones en este aspecto, y puede querellarse cualquier persona víctima de estas conductas. En este punto es importante destacar que los delitos informáticos son delitos de acción pública, lo que significa que no se requiere la existencia de un querellante para que se proceda a iniciar la respectiva investigación y posterior juicio, basta la denuncia y los fiscales están obligados a investigar y perseguir la responsabilidad penal.