FIHS
ABOGADOS

INFORME

LEY N° 21.459

SOBRE DELITOS INFORMÁTICOS

Este 20 de junio de 2022, se publicó en el Diario Oficial la Ley Nº 21.459 sobre delitos informáticos, para actualizar nuestra legislación en estas materias y adecuarla al Convenio de Budapest sobre delitos cibernéticos, ratificado por Chile el año 2017.

Esta legislación era muy esperada, toda vez que la que hasta ahora tipificaba estos delitos en Chile (Ley Nº 19.223) venía desde el año 1993, cuando la realidad tecnológica era diametralmente distinta a la que conocemos hoy. Esto provocaba que muchas situaciones que a todas luces eran ilícitas y afectaban bienes jurídicos dignos de protección, no pudieran ser sancionadas penalmente, lo que partir de la entrada en vigencia de esta ley debería cambiar.

Por otra parte, los delitos contemplados en esta nueva ley pasan a formar parte de aquellos que de acuerdo a la Ley Nº 20.393 generan responsabilidad penal a las personas jurídicas, lo que las obliga a actualizar sus modelos de prevención de delitos, ya que por ellos podrán responder no solo las personas naturales que los hayan cometido, sino que también las personas jurídicas en cuyo seno y en cuyo beneficio se hayan perpetrado. Del mismo modo, sus delitos pasan a ser delitos base del lavado de activos regulado en la Ley Nº 19.913 que crea a la Unidad de Análisis Financiero (UAF).

En cuanto a los nuevos delitos incluidos en esta ley, son los siguientes:

1. Ataque a la integridad de un sistema informático (art. 1°): Obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

2. Acceso ilícito (art. 2°): Sin autorización o excediendo la que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceder a un sistema informático. Aumenta la pena si el acceso es realizado con ánimo de apoderamiento o uso de la información, aplicándose también a quien la divulgue.

3. Interceptación ilícita (art. 3°): Indebidamente interceptar, interrumpir o interferir, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. Aumenta la pena para el que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos.

4. Ataque a la integridad de los datos informáticos (art. 4°): Indebidamente alterar, dañar o suprimir datos informáticos, causando un daño grave al titular de los mismos.

5. Falsificación informática (art. 5°): Indebidamente introducir, alterar, dañar o suprimir datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos. Aumenta la pena si es cometido por empleado público, abusando de su oficio.

6. Receptación de datos informáticos (art. 6°): Conociendo su origen o no pudiendo menos que conocerlo, comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°.

7. Fraude informático (art. 7°): Causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático. Se considera también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta señalada, facilita los medios con que se comete el delito.

8. Abuso de los dispositivos (art. 8°): El que para la perpetración de los delitos de los artículos 1° a 4° de esta ley o del delito de uso fraudulento de tarjetas de pago y transacciones electrónicas del art. 7° de la Ley N° 20.009, entregue u obtenga para su utilización, importe, difunda o realice otra forma de puesta a disposición 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 dichos delitos.

Las penas privativas de libertad de los delitos señalados van desde el presidio menor en su grado mínimo (61 a 540 días) a presidio mayor en su grado mínimo (5 años y 1 día a 10 años). Las de multas llegan hasta las 30 UTM.

Señala qué debe entenderse por “datos y sistemas informáticos” y por “prestadores de servicios”.

En cuanto a circunstancias modificatorias de responsabilidad penal, establece una circunstancia atenuante especial de cooperación eficaz, indicando en qué consiste, así como los requisitos para que opere. Y dos circunstancias agravantes consistentes en cometer el delito abusando de una posición de confianza en la administración del sistema informático, o cometerlo abusando de la vulnerabilidad, confianza o desconocimiento de niños, adolescentes o adultos mayores. Agrega que si como resultado de los delitos se afecta o interrumpe la provisión o prestación de servicios de utilidad pública (ej. electricidad, agua, gas, etc.) o el normal desenvolvimiento de los procesos electorales, la pena correspondiente se aumentará en un grado.

En temas del procedimiento penal, establece: a) que cuando los delitos interrumpan el normal funcionamiento de un servicio de utilidad pública, las investigaciones también podrán iniciarse por querella del Ministro del Interior y Seguridad Pública, así como de los delegados presidenciales regionales y provinciales; b) que en los casos que se señalan en la ley, se permite al Ministerio Público solicitar al Juez de Garantía el uso de las técnicas de interceptación de comunicaciones previstas en los artículos 222 al 226 del CPP, permitiendo incluso la figura del agente encubierto; c) normas especiales en materia de comiso; d) que se permite al Ministerio Público requerir a cualquier proveedor de servicio la conservación o protección de datos informáticos hasta que se obtenga la respectiva autorización judicial para su entrega.

Modifica también el artículo 36 b) de la Ley Nº 18.168 General de Telecomunicaciones incorporando como delito la nueva letra f) que sanciona a los que vulneren el deber de reserva o secreto previsto en los artículos 218 bis, 219 y 222 del CPP, mediante el acceso, almacenamiento o difusión de los antecedentes o la información señalados en dichas normas.

Finalmente, en sus artículos transitorios establece algunas reglas especiales en materia de aplicación de la ley en el tiempo y señala que las modificaciones a las Leyes Nº 20.393 sobre responsabilidad penal de las personas jurídicas y Nº 19.913 de la UAF comenzarán a regir una vez transcurridos 6 meses desde la publicación de esta ley, es decir, a partir del 20 de diciembre de 2022.

Es cuanto puedo informar.

SERGIO HUIDOBRO M.
ABOGADO

Stgo., junio 2022.