alerta legal

Nueva Ley de Delitos Informáticos

El 20 de junio pasado se publicó la Ley N°21.459 (“Ley”), que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, ratificado por Chile el año 2017.

Lo anterior significa una importante actualización en nuestra legislación local en materia de cibercriminalidad, sobre todo si consideramos que la Ley N°19.223, que tipificaba delitos informáticos (espionaje, fraude informático), databa del año 1993. La antigüedad de la ley derogada, no solo implicaba su escasa aplicabilidad práctica producto de que los avances tecnológicos hacían muy difícil su adecuación a las formas de comisión de los delitos en la actualidad, sino que además, presentaba una serie de dificultades procesales, como por ejemplo, la determinación de los tribunales competentes por la dificultad de poder localizar el lugar de comienzo de ejecución del delito, originando muchas veces la impunidad de infracciones cometidas contra chilenos desde el extranjero.

Otro de los aspectos relevantes de la nueva Ley, es que incorpora ocho nuevos delitos (informáticos) a la Ley N°20.393 sobre Responsabilidad Penal de las Personas Jurídicas. Someramente, estos delitos son:

1. Ataque a la Integridad de un sistema informático: Sanciona a quien obstaculice o impida 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. Por ejemplo, la alteración de sistemas informáticos que hacen funcionar los sistemas de transporte, financieros o telecomunicaciones, entre otros.

2. Acceso Ilícito: Sanciona al que, sin autorización, excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático. Cometerá también este delito quien divulgue la información, si no hubiese sido obtenida por éste.

3. Interceptación ilícita: Sanciona al que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. Ejemplo email, o WhatsApp.

4. Ataque a la integridad de los datos informáticos: Sanciona cuando indebidamente se altere, dañe o suprima datos informáticos causando un grave daño al titular de los mismos.

5. Falsificación Informática: Sanciona al que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, como por ejemplo, phishing.

6. Receptación de datos informáticos: Sanciona al que 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 algunos de los delitos descritos en la Ley.

7. Fraude informático: Sanciona a quien, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule 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.

8. Abuso de dispositivos: Sanciona a quien, para la perpetración de determinados delitos previstos en la Ley, entregare u obtuviere para su utilización, importare, difundiera o realizare 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. Por ejemplo, mecanismos para clonar tarjetas de crédito, copiar bandas magnéticas o de sistemas de acceso restringido, etc.

Si bien la incorporación de estos delitos en la Ley 20.393 será a partir del 20 de diciembre próximo, es fundamental que las empresas comiencen desde ya un proceso de revisión de sus estándares de seguridad informática y manejo de información, lo que implica la actualización de los manuales de prevención de delitos y la adopción de medidas concretas en capacitación y procesos internos con el objeto de para minimizar los riesgos de comisión de delitos informáticos dentro de las organizaciones.

CONTACTO

PEDRO PELLEGRINI
ppellegrini@guerrero.cl

DIEGO MORANDÉ
dmorande@guerrero.cl

ALEJANDRA LEITON
aleiton@guerrero.cl