ECIJA OTERO
Av. Apoquindo 3669, Piso 13,
Las Condes, Santiago - Chile
Tel: +562 2361 8900
www.ecija.com

Aprobada nueva ley de delitos informáticos

Con fecha 20 de junio de 2022, se ha promulgado la nueva ley N° 21.459, la cual establece normas sobre delitos informáticos y deroga la ley N° 19.223, modificando a su vez otros cuerpos legales.

La nueva normativa, cuyo proyecto se inició en 2018, tiene como objetivo adecuar la legislación al convenio de Budapest suscrito por Chile, el cual es un acuerdo internacional que busca equiparar en todos los países miembros los tipos penales para los delitos informáticos. La finalidad es lograr que los ciberdelincuentes, que suelen operar desde un país tercero, puedan ser perseguidos a nivel transnacional.

Entre los aspectos a destacar de la nueva ley se encuentran los siguientes:

I. Autorización e investigación académica o Hacking Ético: El artículo 16 de la nueva ley introduce una excepción al acceso ilícito definido por el artículo 2, considerando que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.

II. Tipos penales: Actualiza la tipificación penal de los delitos informáticos que no se regulaban en la normativa anterior. Entre ellos se encuentran los siguientes:
   - Acceso ilícito (art. 2): El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.
   - Interceptación ilícita (art. 3): El 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. Se aumenta la pena para el caso de aquel 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.
   - Ataque a la integridad de los datos informáticos (art. 4): El que indebidamente altere, dañe o suprima datos informáticos.
   - Falsificación informática (art. 5): El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos. La pena será mayor para los casos en que sea un empleado público quién incurra en dicha conducta.
   - Receptación de datos informáticos (art. 6): El 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 las conductas descritas en los artículos 2°, 3° y 5°.
   - Fraude informático (art. 7): El que, 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. La pena impuesta dependerá del valor del perjuicio causado.

- Abuso de los dispositivos (art. 8): El que para la perpetración de los delitos previstos en los artículos 1° a 4° de la ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009 (uso fraudulento de tarjetas de pago y transacciones electrónicas), 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.

III. Circunstancia atenuante especial (art. 9): Será atenuante de responsabilidad penal y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad.

IV. Circunstancias agravantes (art. 10): Serán circunstancias agravantes de los delitos de la nueva ley:
   - Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, debido al ejercicio de un cargo o función.
   - Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.
   - La pena aumentará si se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley N° 18.700.

V. Modificación de otros cuerpos legales, como el Código Procesal Penal, la Ley N° 19.913, que crea la Unidad de Análisis Financiero, la Ley N° 18.168 General de Telecomunicaciones y la Ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos.

VI. Respecto a la entrada en vigor de la nueva ley, se determina que será desde su promulgación en el Diario Oficial, exceptuando, por un lado, lo que afecta al Código Procesal Penal, que aplicará seis meses desde la promulgación de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, y por otro, respecto de los nuevos delitos de lavado de activos, que regirán transcurridos seis meses desde la publicación de la nueva ley en el Diario Oficial.