

Nueva Ley de Delitos Informáticos: aspectos penales y de compliance

Con fecha 20 de junio de 2022, se promulgó la Ley N° 21.459 (en adelante, la “Nueva Ley”) que deroga la Ley N°19.223 (la cual tipificaba figuras penales relativas a la informática) e incluyó una serie de modificaciones legales en materia de delitos informáticos con el objeto de adecuarlos al Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el “Convenio de Budapest”.

Una de las principales novedades de la Nueva Ley constituye la modernización de los tipos penales para adecuarlos a las nuevas formas de comisión de los delitos informáticos y a los avances de la tecnología, en consideración a los nuevos riesgos y ataques sobre bienes jurídicos relevantes que no estaban contemplados en la anterior legislación.

Así, entre otros, es posible apreciar el establecimiento de tipos penales destinados a sancionar expresamente el acceso ilícito a un sistema de información (sin exigir un determinado propósito, art. 2°), el ataque a la integridad de un sistema informático o para afectar su normal funcionamiento (art. 1°), así como también la interceptación ilícita de información (art. 3°) y, en su caso, el ataque a la integridad de éstos (art. 4°). A su vez, se incluye expresamente la figura de fraude informático (art. 7°), lo que permitirá sancionar aquellas estafas cometidas mediante medios electrónicos que antes sólo se podían reconducir parcialmente a las figuras generales de fraude (art. 7°), así como también se sanciona de manera separada la falsificación informática con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos (art. 5°).

Entre las figuras delictivas novedosas, se incluyó la “receptación de datos informáticos” (art. 6°), la cual castiga a aquel que comercialice, transfiera o almacene, a cualquier título, datos informáticos, conociendo o no pudiendo menos que conocer el origen ilícito, es decir, proveniente de algunos de los delitos descritos en la ley. Además, se incluye la figura de abuso de los dispositivos (art. 8°).

Todos los delitos informáticos que se establecen en esta ley se sumarán al catálogo de delitos precedentes de lavado de activos, según las disposiciones de la Ley N° 19.913 que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos.

Del mismo modo, la nueva ley regula expresamente el denominado “hacking ético” que exime de responsabilidad penal al 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 (art. 16°).

Adicionalmente, se incluye la figura de cooperación eficaz como una atenuante de la responsabilidad, es decir, se le permitirá rebajar la pena que se le imponga hasta en un grado a quien entregue información que permita esclarecer los hechos, identificar a los responsables o impida o prevenga la perpetración de alguno de estos delitos. Por otro lado, también se incluyen medidas especiales de investigación, como el uso de agentes encubiertos (art. 12°).

La nueva ley establece asimismo reglas en virtud de las cuales el Ministerio Público puede requerir información, con o sin autorización judicial según las diversas situaciones reguladas, a las empresas prestadoras de servicios de comunicaciones, quienes no sólo adquieren deberes de conservación de la información que mantienen en su poder, sino que adicionalmente deberes de reserva cuya infracción se sanciona con las penas establecidas en el artículo 36 B de la Ley N° 18.168, General de Telecomunicaciones.

Cabe consignar que los delitos informáticos descritos anteriormente darán lugar a la responsabilidad penal de la persona jurídica, al incluirse en el catálogo de delitos base de la Ley N° 20.393. Así, las empresas y personas jurídicas deberán identificar las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de los delitos informáticos e implementar protocolos, políticas y procedimientos específicos que permitan prevenir la comisión de los mencionados delitos. Para estos efectos, tendrán que realizar un levantamiento de riesgos que cubra estos nuevos escenarios de riesgo y actualizar sus respectivas matrices de riesgos y controles de sus Modelos de Prevención de Delitos.

Finalmente, se debe tener en cuenta que la Nueva Ley establece una vigencia diferida. En lo referente a la nueva regulación del Código Procesal Penal, la Nueva Ley señala que comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el Ministro del Interior y Seguridad Pública. Respecto de los nuevos delitos precedentes de lavado de activos como respecto de los nuevos delitos base que se incorporan al catálogo

de la Ley N° 20.393, la Nueva Ley señala que comenzará a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial. Respecto al resto de las disposiciones, especialmente los delitos informáticos, la Nueva Ley entrará en vigor una vez que se publique el decreto promulgatorio en el Diario Oficial.

Autores: Rodrigo Aldoney; Eduardo Alcaíno