Nueva Ley de Delitos Informáticos y sus implicancias para el Compliance

Compliance

Tras una larga espera, el 20 de junio de 2022 se publicó la Ley N°21.459 que establece normas sobre delitos informáticos (la "Ley"), derogando la Ley N°19.223 que regulaba la materia desde 1993. Asimismo, la Ley modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest e incorpora nuevos delitos que tienen por objeto proteger distintos bienes jurídicos como son la privacidad, la propiedad intelectual, la seguridad nacional y la confidencialidad de los sistemas informáticos.

De este modo, los delitos que se incorporan a nuestra legislación son los siguientes:

1. **Ataque a la integridad de un sistema informático**. Consiste en obstaculizar o impedir el normal funcionamiento (total o parcialmente) de un sistema informático. Se comete a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos. Por ejemplo, ransomware, esto es, un malware que impide a los usuarios acceder a sus sistemas o archivos, exigiendo el pago de un rescate para recuperar el acceso.

2. **Acceso ilícito**. Consiste en acceder a un sistema informático superando barreras técnicas o medidas tecnológicas de seguridad, sin autorización o excediendo la autorización que se posee. Por ejemplo, el uso de credenciales de acceso ajenas sin autorización y obtenidas superando barreras técnicas de seguridad.

3. **Interceptación ilícita**. Consiste en interceptar, interrumpir o interferir la transmisión no pública de información en un sistema informático o entre dos o más sistemas informáticos, de forma indebida; o captar, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas que de éstos provienen. Por ejemplo, sniffing, en virtud del cual se realiza una interceptación de datos mediante la captura del tráfico de la red utilizando un sniffer de paquetes para leer los datos que no estén encriptados.

4. **Ataque a la integridad de los datos informáticos**. Consiste en alterar, dañar o suprimir datos informáticos, causando un daño grave al titular de

Av. Apoquindo 3500, Piso 16, Las Condes, Santiago Chile CP7550105 | Teléfono (562) 2307 0900

los mismos, de forma indebida. Por ejemplo, adware, esto es, un malware diseñado para mostrar anuncios en la pantalla, generando beneficios para el programador, pudiendo hacer que el dispositivo ejecute tareas no deseadas.

5. **Falsificación informática**. Consiste en introducir, alterar, dañar o suprimir datos informáticos con la intención de que sean tomados como auténticos o de que sean utilizados para generar documentos auténticos, de forma indebida. Por ejemplo, spoofing, esto es, una actividad maliciosa en virtud de la cual un tercero se hace pasar por una entidad distinta, a través de la falsificación de los datos en una comunicación.

6. **Receptación de datos informáticos**. Consiste en comercializar, transferir o almacenar a cualquier título, datos informáticos provenientes de acceso ilícito, interceptación ilícita o falsificación informática, conociendo o no pudiendo menos que conocer el origen ilícito de dichos datos. Por ejemplo, almacenar una base de datos obtenida a través de un acceso ilícito de otro sistema informático.

7. **Fraude informático**. Consiste en manipular un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos, o a través de cualquier interferencia en el funcionamiento del sistema informático, causando, por una parte, un perjuicio, y por otra, un beneficio propio o para un tercero. Por ejemplo, phishing, esto es, engañar a una persona para que comparta información confidencial a través de suplantaciones de identidad; o el pharming, que consiste en redirigir el tráfico de red a un sitio web fraudulento.

8. **Abuso de los dispositivos**. Consiste en entregar u obtener para su utilización, importar, difundir o realizar otra forma de puesta a disposición de uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso, para la perpetración de los delitos de: ataque a la integridad de sistemas informáticos, acceso ilícito, interceptación ilícita o ataque a la integridad de los datos informáticos. Por ejemplo, copia ilegal de información.

Otra de las novedades de la Ley es la incorporación de estos delitos al catálogo del artículo 1 de la Ley N°20.393 que establece la responsabilidad penal de las personas jurídicas. Lo anterior, implica que las empresas deberán adaptar y actualizar sus Modelos de Prevención de Delitos para incorporar las actividades o procesos, habituales o esporádicos, en cuyo contexto se genere o incrementen los riesgos asociados, así como nuevos protocolos, reglas, procedimientos y controles para evitar que estos delitos se cometan al interior de la organización.

Cabe destacar que estas tipificaciones, principalmente, buscan proteger los intereses de las empresas, ya que en general, son éstas las que se posicionan como víctimas de estos delitos, más que autoras de los mismos. Sin embargo, algunos delitos como, por ejemplo, el nuevo delito de receptación de datos informáticos, sí implican una mayor exposición al riesgo, por lo que el análisis no debe prescindirse, siendo necesario y relevante de cara a la prevención y protección de datos de la propia empresa, sus colaboradores y sus clientes.

Si bien la Ley rige desde su publicación para las personas naturales, se ha establecido un período de vacancia de seis meses para realizar el análisis y las modificaciones en los Modelos de Prevención de Delitos. Por ello, es importante que durante este período las empresas comiencen a analizar sus riesgos relacionados a los delitos informáticos expuestos. Asimismo, se debe poner atención a las distintas actividades donde se administren y resguarden datos y sistemas informáticos, de manera de preparar y aplicar, con anticipación, las medidas de control y políticas de prevención que sean necesarias para mitigar los riesgos asociados a esta nueva Ley.

Av. Apoquindo 3500, Piso 16, Las Condes, Santiago Chile CP7550105 | Teléfono (562) 2307 0900