Boletín N° 18.370-25

Proyecto de ley, iniciado en Moción de los Honorables Senadores señoras Núñez y Órdenes, y señores Castro, Flores y Longton, que modifica la ley N° 21.459, con el objeto de actualizar la regulación en materia de delitos informáticos.

La ley N.° 21.459 significó un avance sustantivo en la adecuación de la legislación chilena al Convenio de Budapest sobre Ciberdelincuencia, reemplazando un marco normativo insuficiente frente a la evolución tecnológica y estableciendo una. tipificación moderna de los principales delitos informáticos.

Sin embargo, la experiencia reciente demuestra que la amenaza ha seguido mutando con rapidez. Los ataques ya no se limitan al acceso ilícito, la interceptación o la alteración de sistemas. Hoy se observan modalidades criminales altamente organizadas, con capacidad transnacional, uso de infraestructura digital distribuida, exigencias de pago mediante activos virtuales, cifrado malicioso de información, destrucción deliberada de respaldos, amenazas de filtración de datos y afectación de servicios esenciales.

Especial preocupación generan los ataques de ransomware y extorsión digital. En estos casos, los delincuentes no sólo bloquean o cifran información, sino que paralizan operaciones, amenazan con divulgar datos sensibles, exigen pagos mediante criptoactivos o utilizan redes de anonimización, intermediarios digitales y plataformas extranjeras para dificultar la trazabilidad de los responsables.

A ello se suma una modalidad particularmente grave: la destrucción maliciosa de datos o sistemas informáticos, conocida internacionalmente como wiping o destrucción digital. Esta conducta puede perseguir la eliminación de evidencia, la interrupción de servicios, la afectación de La continuidad operacional o la imposibilidad de recuperación de información crítica. Su impacto puede ser especialmente severo cuando afecta hospitales, servicios públicos, entidades financieras, telecomunicaciones, transporte, energía, agua potable, puertos, aeropuertos, procesos electorales, seguridad pública o defensa nacional.

La legislación penal debe ser capaz de distinguir entre ataques informáticos comunes y conductas que comprometen bienes jurídicos de mayor entidad, como la continuidad de servicios esenciales, la seguridad pública, la integridad de infraestructura crítica, la confianza en los sistemas financieros, la protección de datos estratégicos del Estado y el normal funcionamiento de instituciones públicas y privadas indispensables para la vida nacional.

El proyecto no pretende sustituir la arquitectura general de la ley N.° 21.459, sino

complementaria en aquellos puntos donde la práctica criminal evidencia nuevas brechas. En particular, se propone incorporar tipos penales específicos para la destrucción maliciosa de datos o sistemas informáticos y para el secuestro de datos y extorsión digital, reforzar las reglas de agravación cuando se afecten servicios esenciales o infraestructura crítica, y reconocer expresamente la dimensión económica de estos delitos mediante reglas de comiso y medidas cautelares sobre activos digitales.

Asimismo, se establece una regulación más precisa sobre preservación reforzada de evidencia digital, cadena de custodia digital, coordinación técnica con la Agencia Nacional de Ciberseguridad y cooperación internacional en materia de evidencia electrónica transfronteriza. Estas herramientas son indispensables porque, en el entorno digital, la evidencia puede ser eliminada, cifrada, transferida o alojada fuera del territorio nacional en cuestión de minutos.

Chile es parte del Convenio de Budapest sobre Ciberdelincuencia, instrumento internacional que constituye el principal estándar multilateral en materia de delitos informáticos, cooperación penal internacional y evidencia electrónica.

Además, Chile suscribió el Segundo Protocolo Adicional al Convenio de Budapest, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. Dicho instrumento apunta precisamente a mejorar la cooperación internacional, facilitar la preservación y obtención de evidencia electrónica, habilitar mecanismos más expeditos de cooperación con proveedores de servicios y reforzar la respuesta frente a investigaciones transfronterizas, siempre bajo resguardos de legalidad, proporcionalidad, protección de datos personales y respeto de los derechos fundamentales.

La presente iniciativa se inspira en esa evolución internacional. En particular, reconoce que la persecución penal de la ciberdelincuencia requiere mecanismos eficaces para preservar evidencia, identificar responsables, rastrear infraestructura digital, coordinar diligencias internacionales y evitar que la localización extranjera de datos, servidores, plataformas o proveedores se transforme en una barrera de impunidad.

La dictación de la ley N.° 21.663, Marco de Ciberseguridad, incorporó al ordenamiento jurídico chileno categorías relevantes como los servicios esenciales, los operadores de importancia vital y la Agencia Nacional de Ciberseguridad. Ello exige una armonización entre la respuesta administrativa en materia de ciberseguridad y la respuesta penal frente a ataques informáticos graves.

No basta con sancionar el daño informático en abstracto. La ley debe reconocer que un mismo ataque puede tener consecuencias muy distintas si afecta un computador particular, una

empresa común, un hospital, un puerto, un servicio financiero, una red de telecomunicaciones, un sistema eléctrico, un proceso electoral o una infraestructura vinculada a la defensa nacional.

Por ello, el proyecto incorpora reglas especiales de agravación cuando la conducta afecte servicios esenciales, operadores de importancia vital, infraestructura crítica de la información o sistemas de relevancia pública. Esta diferenciación permite una respuesta penal proporcional al daño potencial o efectivo producido por el ataque.

La persecución moderna de los delitos informáticos exige hacerse cargo de tres problemas prácticos.

Primero, la evidencia digital es frágil, volátil y fácilmente transferible. Por ello se requiere fortalecer las reglas de preservación inmediata, trazabilidad, cadena de custodia, análisis forense y tratamiento de información alojada en la nube o en jurisdicciones extranjeras.

Segundo, muchos ataques informáticos tienen finalidad económica y se ejecutan mediante pagos en activos virtuales, billeteras digitales, cuentas de intercambio, intermediarios tecnológicos y mecanismos de ocultamiento patrimonial. Por esa razón, el proyecto incorpora reglas expresas sobre comiso de activos virtuales, comiso por valor equivalente y medidas cautelares destinadas a inmovilizar o preservar bienes digitales vinculados al delito.

Tercero, una parte relevante de la ciberdelincuencia contemporánea no responde a actuaciones individuales aisladas, sino a estructuras organizadas, permanentes y transnacionales. En consecuencia, se permite que el tribunal considere especialmente la comisión de estos delitos en contextos de asociación u organización criminal, sin perjuicio de las responsabilidades penales que correspondan conforme a la legislación.

El proyecto mantiene como principio rector que toda medida de investigación, preservación, cooperación internacional, acceso a información, incautación, análisis de evidencia o afectación patrimonial debe sujetarse a la Constitución, a la ley, al control judicial cuando corresponda, al principio de proporcionalidad, a la protección de datos personales, al secreto profesional y a los tratados internacionales vigentes.

La finalidad de la iniciativa no es ampliar indiscriminadamente las facultades intrusivas del Estado, sino dotar al sistema penal de herramientas específicas, proporcionales y técnicamente adecuadas para enfrentar delitos que, por su velocidad, anonimato, sofisticación y dimensión transnacional, requieren una respuesta más eficaz.

En definitiva, la presente reforma busca cerrar brechas normativas, actualizar la persecución penal frente al ransomware y la extorsión digital, proteger servicios esenciales e

infraestructura crítica, fortalecer la cooperación internacional y asegurar que la evidencia electrónica y los activos digitales puedan ser preservados, analizados y sometidos al control de los tribunales conforme a las garantías propias de un Estado de Derecho.

IDEA MATRIZ

El proyecto tiene por objeto modernizar la legislación penal sobre delitos informáticos, fortaleciendo la persecución del ransomware, la extorsión digital, la destrucción maliciosa de datos, la afectación de infraestructura crítica, la preservación de evidencia electrónica, la cooperación internacional y el comiso de activos virtuales.

PROYECTO DE LEY

Modifica la ley N.° 21.459, con el objeto de fortalecer la persecución del secuestro de datos, la extorsión digital, la afectación de servicios esenciales y operadores de importancia vital, y la preservación de evidencia digital.

Artículo único. - Introdúcense las siguientes modificaciones en la ley N.° 21.459, que establece normas sobre delitos informáticos:

1. Incorporase el siguiente artículo 7 bis:

"Artículo 7 bis. - Secuestro de datos y extorsión digital. El que, mediante cifrado, bloqueo, alteración, supresión, inutilización, restricción de acceso, amenaza de divulgación o cualquier otra forma de afectación maliciosa de datos informáticos o sistemas informáticos, exigiere para sí o para un tercero dinero, activos virtuales, criptoactivos, prestaciones, abstenciones o cualquier otro beneficio económico, será sancionado con presidio mayor en su grado mínimo y multa de cincuenta a quinientas unidades tributarias mensuales.

La misma pena se aplicará a quien, habiendo obtenido ilícitamente datos informáticos, amenazare con divulgarlos, transferirlos, venderlos, destruirlos o mantenerlos inaccesibles con el objeto de obtener un beneficio económico.
No impedirá la configuración del delito que la exigencia se formule mediante activos virtuales, plataformas extranjeras, redes de anonimización, cuentas de terceros, intermediarios digitales, sistemas automatizados u otros mecanismos destinados a dificultar la identificación del responsable, la trazabilidad del pago o la recuperación de la información.

Si la conducta afectare servicios esenciales, operadores de importancia vital o infraestructura crítica de la información, en los términos previstos en la ley N.° 21.663, la pena será de presidio mayor en sus grados mínimo a medio.".

2. Reemplázase el inciso final del artículo 10 por el siguiente:

“Si como consecuencia de las conductas previstas en esta ley se afectare, interrumpiere, degradare, alterare o pusiere en riesgo relevante la continuidad, seguridad, integridad o disponibilidad de servicios esenciales, operadores de importancia vital o infraestructura crítica de la información, en los términos previstos en la ley N.° 21.663, la pena correspondiente se aumentará en un grado.

Cuando la afectación produjere daño masivo, interrupción prolongada, riesgo para la vida o salud de las personas, paralización relevante de la actividad económica, compromiso grave de datos estratégicos del Estado o afectación sustantiva de la seguridad nacional, el aumento será de dos grados.

En los casos del inciso anterior, la pena aplicable no podrá ser inferior a presidio mayor en su grado mínimo.”.

3. Incorporase el siguiente artículo 12 bis:

“Artículo 12 bis.- Preservación urgente de evidencia digital. Cuando existieren antecedentes fundados de que datos informáticos, registros de conexion, credenciales, trazas técnicas, direcciones IP, nombres de dominio, servidores, cuentas, dispositivos, respaldos, billeteras digitales, activos virtuales u otros antecedentes electrónicos vinculados a alguno de los delitos previstos en esta ley pudieren ser alterados, eliminados, ocultados, cifrados, transferidos o trasladados fuera del territorio nacional, el Ministerio Público podrá requerir su preservación inmediata por un plazo de noventa días, prorrogable por una sola vez.

La preservación sólo tendrá por objeto impedir la pérdida, alteración o indisponibilidad de los antecedentes requeridos, y no habilitará por sí sola su entrega, acceso, apertura, registro, incautación o análisis, actuaciones que deberán sujetarse a la autorización judicial previa cuando corresponda conforme a la ley.

Las personas naturales o jurídicas que tuvieren bajo su control los antecedentes requeridos deberán adoptar medidas razonables para asegurar su conservación íntegra, trazable y verificable durante el plazo respectivo.

La aplicación de este artículo deberá respetar las garantías constitucionales, el principio de proporcionalidad, la protección de datos personales, el secreto profesional, la reserva legalmente procedente y los tratados internacionales vigentes.”

4. Incorporase el siguiente artículo 12 ter:

“Artículo 12 ter.- Coordinación técnica especializada. En investigaciones por delitos previstos

en esta ley que afectaren servicios esenciales, operadores de importancia vital o infraestructura crítica de la información, en los términos previstos en la ley N.° 21.663, el Ministerio Público podrá requerir antecedentes técnicos, informes especializados, indicadores de compromiso, análisis de riesgo o apoyo técnico de la Agencia Nacional de Ciberseguridad u otros organismos públicos competentes, conforme a sus respectivas atribuciones legales.

La intervención de dichos organismos tendrá carácter técnico y colaborativo, no afectará la dirección exclusiva de la investigación penal que corresponde al Ministerio Público ni podrá importar el ejercicio de facultades investigativas autónomas.

La información obtenida en virtud de este artículo deberá utilizarse para los fines de la investigación respectiva, sin perjuicio de las competencias administrativas que correspondan conforme a la ley N.° 21.663 y demás normas aplicables. Dicha información conservará la reserva o confidencialidad que le otorgue la legislación especial.”.

5. Incorporase el siguiente artículo 13 bis:

“Artículo 13 bis.- Comiso de activos virtuales y ganancias derivadas de delitos informáticos. Sin perjuicio de las reglas generales sobre comiso, comiso de ganancias y comiso por valor equivalente previstas en la legislación vigente, en los delitos contemplados en esta ley caerán especialmente en comiso los activos virtuales, criptoactivos, tokens, billeteras digitales, claves de acceso, llaves criptográficas, cuentas de intercambio, instrumentos tecnológicos, beneficios económicos y cualquier utilidad obtenida directa o indirectamente con ocasión del delito.

El comiso procederá aun cuando dichos bienes hubieren sido convertidos, transformados, mezclados, transferidos, fraccionados o mantenidos bajo el control de terceros, salvo respecto de quienes acreditaren haber actuado de buena fe y a título oneroso.

Cuando los bienes no pudieren ser habidos, el tribunal podrá decretar el comiso por valor equivalente respecto de otros bienes del condenado, hasta el monto del beneficio económico obtenido.”.

6. Incorporase el siguiente artículo 13 ter:

“Artículo 13 ter.- Medidas cautelares sobre activos digitales. Durante la investigación, el Ministerio Público podrá solicitar al juez de garantía medidas cautelares destinadas a inmovilizar, congelar, bloquear, preservar o impedir la transferencia de activos virtuales, billeteras digitales, cuentas de intercambio, instrumentos financieros digitales, dominios, servidores, credenciales u otros activos susceptibles de movilización electrónica, cuando existieren antecedentes fundados de que provienen de alguno de los delitos previstos en esta

ley, han servido para su comisión o corresponden a ganancias derivadas del mismo.

Estas medidas deberán ser fundadas, proporcionales, limitadas temporalmente y sujetas a revisión judicial. En lo no regulado por este artículo se aplicarán las reglas generales del Código Procesal Penal y demás legislación pertinente.”.

7. Incorporase el siguiente artículo 14 bis:

“Artículo 14 bis.- Cadena de custodia digital. Los antecedentes electrónicos, datos informáticos, registros técnicos, evidencias provenientes de sistemas en la nube, activos virtuales, dispositivos, servidores, respaldos, credenciales, imágenes forenses, trazas de comunicación y demás elementos digitales de investigación deberán ser preservados conforme a estándares de integridad, autenticidad, trazabilidad, reproducibilidad y no alteración.

El Fiscal Nacional podrá dictar instrucciones generales sobre preservación forense, cadena de custodia digital, tratamiento de evidencia en la nube, análisis de activos virtuales, evidencia electrónica transfronteriza y coordinación con organismos técnicos especializados.

Dichas instrucciones promoverán el resguardo de la validez procesal de la evidencia, la protección de datos personales, la reserva de las investigaciones, el secreto profesional cuando corresponda y los derechos fundamentales de las personas.".