MATERIA	**Boletín 12192-25.** Delitos informáticos.
AUTORES	Pablo Viollier
DESTINATARIO	Comisión de Seguridad Pública del Senado
FECHA	03/01/2019

El proyecto busca modificar distintos cuerpos legales con el objetivo de implementar las obligaciones contraídas por Chile al momento de ratificar el Convenio sobre ciberdelincuencia del Consejo de Europa, también conocido como el Convenio de Budapest ("el Convenio"). Si bien el proyecto de ley avanza en distintas áreas de la regulación de delitos informáticos, hay ciertas disposiciones que es necesario corregir, ya sea por razones de técnica legislativa, coherencia con lo dispuesto en el Convenio o por resultar lesivas de los derechos fundamentales de las personas.

1. **Perturbación informática**

El artículo 1° del proyecto tipifica el delito de "perturbación informática". Sin embargo, la figura de la perturbación informática no se encuentra recogida en el Convenio ni en la legislación comparada. Siendo el Convenio una iniciativa para promover la homogeneización de la tipificación de los delitos informáticos a nivel comparado, resultaría más conveniente tipificar de forma separada el ataque a la integridad de los datos y el ataque a la integridad del sistema como se contempla en el Convenio. También resulta relevante señalar que el término "perturbación" resulta excesivamente amplio, dando a entender que cualquier tipo de afectación a un sistema informático, por menor que esta sea, puede constituir una perturbación de este, aún cuando ésta pueda carecer de efectos nocivos para el mismo.

2. **Acceso ilícito**

En cuanto a la tipificación del delito de acceso ilícito, contenida en el artículo 2°, el proyecto sólo exige que este acceso sea cometido de forma indebida, independiente de si se realiza de buena o mala fe, o con la intención de apoderarse o conocer indebidamente la información ahí contenida. Al considerarse el requisito de "indebido" como sinónimo de "sin permiso", **la descripción del tipo puede significar la criminalización de un área clave de la ciberseguridad: la detección de vulnerabilidades en los sistemas informáticos**. De esta forma, un experto en seguridad informática que acceda a un sistema para probar la seguridad de este en búsqueda de vulnerabilidades estará cometiendo una conducta descrita por el artículo 2°, incluso si su actividad es realizada de buena fe y con la intención reportar la vulnerabilidad al administrador del sistema.

El mismo artículo establece que vulnerar, evadir o transgredir medidas de seguridad informática para lograr dicho acceso constituye una agravante para la comisión del delito. Sin embargo, **esta agravante debería ser en realidad un requisito del delito de acceso ilícito, ya que no puede existir un delito informático si el perpetrador no ha superado algún tipo de barrera técnica**. De lo contrario, la simple infracción de una obligación

contractual o de los términos y condiciones de un sitio web pasarían a constituir un delito castigado por la ley.

3. **Utilización de cifrado como agravante de la responsabilidad penal**

Otro elemento del proyecto que requiere ser corregido es el artículo 9°, el que establece que la utilización de tecnologías de cifrado se considerará como un agravante de cualquiera de los delitos contenidos en la ley, en la medida que tenga por principal objetivo obstaculizar la acción de la justicia. Esta exigencia no se encuentra en forma alguna recogida en el Convenio.

Criminalizar el cifrado atenta contra el principio de no incriminación, al sancionar a aquella persona que no colabora con su propia persecución penal. Por otro lado, el cifrado por defecto se ha transformado en el estándar para la industria a nivel global, por lo que en un futuro cercano simplemente será imposible cometer un delito informático sin haber utilizado alguna forma de tecnología que involucre cifrado. Lo anterior implicaría que todos los delitos informáticos estarían -por defecto- agravados por esta causal. Por último la amenaza de incurrir en un delito así tipificado generaría un descintencivo general al uso de cifrado en Chile, poniendo el nivel de ciberseguridad del país por debajo de los estándares internacionales y obligando a proveedores tecnológicos a degradar sus servicios ofrecidos en el país.

4. **Modificación al régimen de retención de datos de tráfico por parte de las empresas proveedoras de servicio de internet.**

El artículo 16° del proyecto modifica el artículo 222 del Código Procesal Penal con el fin de aumentar el período de retención de datos de tráfico y los tipos de datos que deben retener las empresas proveedoras de servicio de internet. De esta forma, el proyecto busca el mismo objetivo que el Decreto Nº866 del Ministerio del Interior o llamado "Decreto Espía" durante el año 2017, iniciativa que la Contraloría General de la República declaró ilegal e inconstitucional.

Las políticas de retención de datos de tráfico han demostrado ser ineficaces para el combate del delito, costosas para la industria, contrarias a los principios de la ciberseguridad y han sido consistentemente cuestionadas en diferentes jurisdicciones alrededor del globo. **Esta iniciativa aumenta de forma desproporcionada la capacidad de vigilancia del Estado e invierte el principio de inocencia, por lo que su implementación resultaría incompatible con el derecho a la protección de la vida privada de la población**, recogido en el artículo 19°4 de nuestra Carta Fundamental. Esta exigencia no se encuentra en forma alguna recogida en el Convenio.

5. **Conclusiones y recomendaciones**

Vale la pena recordar que, durante la tramitación legislativa del Convenio de Budapest, el ejecutivo se comprometió explícitamente a que la implementación de este instrumento no iba a significar un debilitamiento de ningún estándar, derecho o garantía al interior del proceso penal. Algunos parlamentarios incluso condicionaron su voto al cumplimiento de dicho compromiso.

En consecuencia, se sugiere realizar las modificaciones señaladas en la presente minuta al proyecto de ley, de forma tal que este se encuentre en concordancia con las disposiciones del Convenio de Budapest y se subsanen aquellas disposiciones de carácter inconstitucional y que pueden significar una eventual vulneración de los derechos fundamentales de las personas.