Boletín N°10145-07

**Tipifica y sanciona los delitos informáticos y deroga la ley N° 19.223**

1. El proyecto busca actualizar el marco jurídico relativo a los delitos informáticos, proponiendo un nuevo cuerpo normativo que sancione este tipo de conductas antijurídicas, y derogando la Ley N° 19.223 de 1993.

2. El proyecto conserva, en sus aspectos más relevantes, la forma en que la Ley N° 19.223 tipifica los delitos informáticos, y la pena aplicable por dichas conductas. Sin embargo, establece agravantes y modificaciones procesales que son altamente preocupantes para el respeto de los derechos fundamentales en el entorno digital.

3. El delito de *espionaje informático* actualmente exige que la conducta de acceso, interceptación o interferencia se haga con el ánimo de apoderarse, usar o conocer "indebidamente" los datos de un sistema de tratamiento de información. El proyecto elimina dicho requisito, y en cambio, sanciona a quien *"sin derecho acceda o use información contenida en un sistema de tratamiento de datos"*. El proyecto **establece un tipo penal sumamente amplio**, que no exige la vulneración de un sistema informático, y que podría utilizarse para sancionar una serie de conductas legítimas (como la investigación de seguridad), o incluso castigar a quienes actuaron sin una intención dolosa. Esto contrasta con la forma en que el derecho comparado tipifica este delito: las leyes en España y Alemania exigen que el acceso se produzca contra la voluntad del titular, y vulnerando alguna medida de seguridad[1].

4. Por otro lado, el proyecto no subsana una falencia importante de la legislación actual, en que la sanción no distingue ni la clase o importancia de la información ni la forma para acceder a ella, lo que ha sido criticado sostenidamente por la doctrina[2].

5. El proyecto sanciona la tenencia, posesión, producción, venta difusión o cualquier otra forma de puesta a disposición de dispositivos (incluyendo códigos) que permitan la comisión de alguno de estos delitos. No exige que la tenencia, posesión o difusión se realice a sabiendas, y la descripción alcanza a prácticamente cualquier dispositivo moderno. Por tanto, podrían resultar sancionados individuos que no han cometido ninguna conducta ilícita.

6. El artículo 6º permite la interceptación de comunicaciones privadas para investigar estos delitos. Dicha incorporación resulta innecesaria, toda vez que el Código Procesal Penal ya otorga dichas facultades al Ministerio Público, respecto de delitos más graves. El uso de

[1] Ver, MEDINA, Gonzalo (2014). Estructura típica del delito de intromisión informática *Revista Chilena de Derecho y Tecnología*. Vol 3, N°1, p. 89. Disponible en: http://repositorio.uchile.cl/handle/2250/126717

[2] Ver, MOSCOSO, Romina (2014). La Ley 19.223 en general y el delito de *hacking* en particular. *Revista Chilena de Derecho y Tecnología*. Vol 3, N°1, p.16. Disponible en: http://www.rchdt.uchile.cl/index.php/RCHDT/article/view/32220

medidas así de intrusivas no tiene correlación con la penalidad asignada a estos delitos, y no responde a los principios de necesidad y proporcionalidad.

7. El proyecto contempla que la utilización de un medio informático se incorpore como circunstancia agravante para efectos de determinar la responsabilidad penal. La calificación de agravante está reservada para aquellas circunstancias que aumenten lesividad de una conducta. No corresponde que el medio de comisión de un delito sea calificado, en sí mismo, como un agravante de la responsabilidad penal. Se estaría pasando por alto el principio de que nadie puede ser castigado dos veces por la misma conducta (*non bis in idem)*, reconocido en la Constitución. Por otro lado, mientras los Códigos Penales modernos avanzan hacia una neutralidad tecnológica, el proyecto propone transitar el camino contrario.

8. El proyecto modifica el artículo 222 del Código Procesal Penal, que contiene la obligación retención de datos de tráfico (listado actualizado de los números IP y registro de las conexiones que realicen los usuarios). Pretende extender esta obligación a otras instituciones como bancos, establecimientos educacionales, comerciales o que presten servicios de comunicación digital, sin observar lo difícil que es que las instituciones descritas puedan dar cumplimiento a dicha obligación. Por otro lado, se aumenta el tiempo de mantención del registro de uno a **quince años**, lo que resulta altamente desproporcionado y no responde a ningún estándar internacional. No existe evidencia alguna de que esta clase de medidas resulte útil para la prevención del delito. Por el contrario, una medida así ha sido calificada como contraria a los derechos humanos en la Unión Europea[3].

9. Por lo anterior, no cabe sino concluir que el proyecto de ley en cuestión sufre problemas de técnica legislativa, establece tipos penales amplios, sufre de posibles vicios de inconstitucionalidad, y puede resultar altamente perjudicial para la observancia de los derechos fundamentales en el entorno digital.

10. Por último, cabe destacar que el gobierno ya ha hecho oficial su decisión de ratificar el Convenio de Budapest sobre ciberdelincuencia, y un comité interministerial ya se encuentra estudiando como adecuar nuestra legislación a dicho cuerpo internacional. Por lo mismo, la tramitación del presente proyecto de ley puede significar una duplicación de esfuerzos en la materia, y de aprobarse, es probable que sea modificado por la adecuación de nuestra legislación al Convenio de Budapest.

[3] Tribunal de Justicia de la Unión Europea, sentencia en casos C-293/12 y C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 de abril de 2014, que declara nula la Directiva 2006/24/EC del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas.