Francisco Javier Bedecarratz Scholz
Abogado
Magíster y Doctor en Derecho

Minuta exposición
Comisión de Seguridad Ciudadana, Cámara de Diputados, sesión del 28 de septiembre 2020

PROYECTO DE LEY QUE ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST (BOLETÍN N° 12.192-25)

Sumario Ejecutivo

El Proyecto de Ley constituye un claro avance para el cumplimiento del Convenio de Budapest en lo relativo a la sanción de delitos informáticos. No obstante este favorable diagnóstico, son necesarias ciertas precisiones en texto, especialmente en cuanto a la punibilidad del acceso ilícito y sus normas complementarias.

I. Presentación

Por su intermedio señor Presidente, quiero en primer lugar agradecer la cordial invitación que se me ha extendido, para exponer sobre el "Proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest", Boletín N° 12.192-25 (en adelante el "Proyecto"). Conforme a lo anterior, se ha considerado necesario fundamentar previamente si el Proyecto satisface las obligaciones internacionales referentes a los tipos penales incorporados, para luego revisar una norma específica que admitiría modificaciones, con el fin de mejorar su aplicación práctica.

II. Valoración del proyecto

En relación con las obligaciones contraídas por Chile en el ámbito penal, que es el primer punto de esta exposición, es importante destacar que el Proyecto tipifica los delitos de Ataque a la integridad de un sistema informático (art. 1°), Acceso ilícito (art. 2°), Interceptación ilícita (art. 3), Ataque a la integridad de los datos (art. 4), Falsificación informática (art. 5), Receptación de datos (art. 6), Fraude informático (art. 7), y Abuso de dispositivos (art. 8°). Además de las modificaciones de los tipos penales, se incorpora una atenuante especial de cooperación eficaz para el esclarecimiento de hechos investigados (art. 9°), así como diversas agravantes especiales (art. 10°). Por otra parte, se incorpora nueva normativa al Código Procesal Penal, entre las que se pueden destacar normas acerca de querellas por estos delitos (art. 11), medidas especiales de

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

investigación del 222 al 226 del CPP y agentes encubiertos (art. 12), el comiso (art. 13), la preservación provisoria de datos informáticos, así como la entrega de datos y el plazo de retención de estos (art. 18 N°1). Finalmente, se faculta la persecución de personas jurídicas en caso de que sus empleados o directivos cometan estos delitos en beneficio o provecho de la entidad (art. 21).

Circunscribiendo el análisis solamente a los tipos penales, es posible concluir que el Proyecto **constituye un claro avance en el cumplimiento** de los compromisos internacionales contraídos por Chile a través de la firma del Convenio sobre la Ciberdelincuencia. Los tipos penales propuestos poseen una estructura homóloga a los contenidos en el Convenio. Además, exhiben un marco de punibilidad equivalente y, con ello, cumplen idéntica función. Sin perjuicio de lo anterior, el Proyecto admite mejoras en cuanto a ciertos tipos penales, que permitirían precisar los marcos punitivos y mejorar su efectividad práctica. Esta exposición se centrará especialmente en la figura del acceso ilícito.

III. El delito de acceso ilícito

En su actual redacción, el art. 2° del Proyecto sanciona la conducta de acceso a sistemas informáticos sin autorización (o excediendo la que se posea), y superando, al mismo tiempo, barreras de seguridad. De modo general, el acceso no autorizado a un sistema informático lesiona o pone en peligro diversos bienes jurídicos protegidos, particularmente, el derecho a la privacidad del titular del sistema vulnerado. Igualmente, el derecho constitucional a la protección de los datos personales también se ve afectado, al obtenerse acceso a los mismos por un tercero con absoluta infracción a su base fundamental, que es el principio de licitud. Finalmente, existe una puesta en peligro concreta del derecho de propiedad del titular sobre los datos contenidos en el sistema accedido ilícitamente, pues estos últimos pueden ser apropiados, destruidos, modificados o dispuestos de cualquier modo. De esta forma, la norma busca sancionar la puesta en peligro que representa el acceso no autorizado a datos personales o información privada, así como la lesión de la privacidad del titular, a través de una conducta equivalente a una "violación electrónica de morada".

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

En el texto aprobado por el Senado, la conducta punible requiere, antes de ser sancionada, dos requisitos. En primer lugar, el acceso debe ser realizado "superando barreras técnicas o medidas tecnológicas de seguridad" para ser punible. El Convenio faculta expresamente a los Estados miembros incluir este requisito que, en la práctica, reduce el marco de punibilidad de la conducta de acceso ilícito. Lo anterior, pues hace reprochable solamente aquellos accesos que vulneran sistemas resguardados por medidas adicionales de seguridad. Así, se excluye del campo de aplicación a todo tipo de acceso realizado sobre sistemas no protegidos con este tipo de medidas.

En segundo lugar, la norma exige como requisito típico que el acceso se haya efectuado sin autorización o excediendo la que posea el sujeto. Este requisito traduce en nuestro idioma el elemento de "ilegitimidad" exigido por el Convenio. Así, este será ilegítimo, en la medida que no cuente con autorización o sea insuficiente.

1. El art. 16 del PDL como excepción redundante

En cuanto al requisito en comento, el art. 16 del Proyecto dispone que se entenderá que cuenta con autorización, todo aquel que acceda a sistemas informáticos en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, ostentando la autorización expresa del titular respectivo. La norma responde a la preocupación relativa a que la penalización del acceso no autorizado podría restringir, en el ámbito nacional, la investigación de la ciberseguridad y su desarrollo científico futuro. En concordancia con lo anterior, se ha aprobado una disposición que garantizaría la no-punibilidad de este tipo de investigaciones, en tanto se presente un acceso bajo las condiciones enunciadas.

Sin embargo, más allá de la intención de resguardar la investigación y el desarrollo, la disposición no posee un contenido que aporte elementos útiles al fin pretendido. Ello, pues la "autorización" ya se contempla como un **requisito negativo del tipo** en el art. 2° del Proyecto, en el sentido que la conducta de acceso será punible, en tanto no exista autorización del titular para acceder al sistema informático. La norma eximente, además, **exige un consentimiento "expreso"**, mientras que el art. 2° admite un consentimiento tácito y es, por lo tanto, más amplio que la excepción. En suma, el art. 16 es redundante y, no solo ello, inidóneo para lograr el fin propuesto.

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

2. Instituciones sustantivas

El objetivo pretendido, de resguardar la investigación y desarrollo en ciberseguridad, puede ser logrado más efectivamente mediante otras instituciones legales.

En particular, la investigación en seguridad informática, la industria de la ciberseguridad y otras actividades similares, son todas actividades lícitas que, desarrolladas en un marco ético y socialmente aceptable, no son punibles, porque en el fondo buscan resguardar el bien jurídico protegido. Esta es la razón de que todas las figuras del acceso punible sean tipificadas en el Derecho comparado como "tipos abiertos". Es decir, se contempla como requisito expreso la "ilegitimidad" o "ilicitud" de la conducta, obligando al juez valorar desde un punto de vista material y de modo concreto lo que está prohibido. Lo anterior es de especial relevancia, pues permite al juez eximir de pena a aquellas conductas constitutivas de acceso sin autorización formal, pero que al mismo tiempo no son ilícitas, por estimarse necesarias para prevenir un ataque a la integridad de un sistema, por ejemplo.

Como complemento de lo anterior, el art. 10 N° 10 del Código Penal ya establece como exención de responsabilidad el "ejercicio legítimo de un oficio". Esta norma exime de toda pena a aquellas personas que, en el ejercicio de una profesión u oficio, realizan conductas que, objetivamente, están cumpliendo los requisitos de un delito. Lo anterior ocurre comúnmente con abogados, periodistas o médicos que, respectivamente, satisfacen los requisitos típicos de desacato, injurias o lesiones corporales, pero que no pueden ser sancionados. En tal sentido, se ha entendido que la profesión u oficio implica ciertos derechos, que justifican conductas típicas que son necesarias para el ejercicio de la profesión.

En el mismo sentido, el desarrollo de actividades de investigación o económicas en el ámbito de la ciberseguridad, puede operar como causal de justificación frente a la conducta de acceso a sistemas informáticos de terceros, en tanto se sustentan en normas extrapenales que cristalizan la legitimidad de este tipo de conductas. Con todo, especial atención deberá ponerse en la voz "ejercicio legítimo" del oficio, en tanto aquel realizado en transgresión a principios éticos o en vulneración a los derechos de la víctima, jamás podrán justificar la conducta.

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

Concordantemente con lo anterior, la licitud de la investigación y desarrollo en ciberseguridad y las conductas de hacking ético puede ser reforzada estableciendo canales de denuncias y protocolos gubernamentales de divulgación de vulnerabilidades. De tal manera, la investigación en ciberseguridad puede ser validado a través de una solución institucional de gobernanza, que daría transparencia a su funcionamiento y lo validaría socialmente. Esta solución se ha propuesto en noviembre 2019 en USA, y cuenta con general aceptación en ese país.

3. Condición de procesabilidad

Además, una segunda herramienta puede ser el establecer una condición adicional de procesabilidad para este delito. En tal sentido, puede establecerse como presupuesto para iniciar la acción penal respectiva, la denuncia o querella del afectado, calificando de tal modo el delito de acceso ilícito como de acción penal pública previa instancia particular, conforme al art. 54 del Código Procesal Penal. La naturaleza particular de los intereses protegidos por el art. 2° del Proyecto, haría prudente conceder a los afectados el derecho exclusivo de decidir, a través de una denuncia o querella, si el acceso ha vulnerado de modo intolerable sus bienes jurídicos protegidos y si es este merecedor, en consecuencia, de una persecución y sanción penal. La incorporación de esta figura en el catálogo del art. 54 del Código Procesal Penal estaría, por lo demás, en concordancia con los demás delitos contenidos en el mismo, también referidos a la divulgación de información privada, así como violación y comunicación de secretos de distinta índole a terceros. En esta materia, es de toda lógica conceder a los afectados la decisión si la conducta deberá ser perseguida o no.

IV. Consideraciones finales

La conducta sancionada en el art. 2° del Proyecto satisface razonablemente las obligaciones contenidas en el Convenio, en orden a tipificar el delito de acceso ilícito en la legislación nacional. Sin embargo, el art. 16 del Proyecto posee un contenido redundante con el tipo penal del acceso ilícito, que hace aconsejable su eliminación. Por otra parte, la no-criminalización de actividades lícitas, tales como las investigaciones de vulnerabilidad de sistemas o aquellas destinadas a mejorar la seguridad informática, ya se encuentra garantizada a través de las instituciones pertenecientes a la parte general del Derecho penal. Concordantemente, resultaría

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl

ventajoso calificar el delito de acceso ilícito como uno de acción penal pública previa instancia particular según el art. 54 del Código Procesal penal. Por último, la conducta del hacking ético no puede ser objeto de una eximente a la medida, sea esta en la forma de una excusa legal absolutoria o de otra forma. La investigación y desarrollo en ciberseguridad, debe ser regulada a través de una normativa que establezca derechos y obligaciones claras en su ejercicio.

Avenida Pedro de Valdivia 425, Providencia, Santiago
Correo electrónico: francisco.bedecarratz@uautonoma.cl