Francisco Javier Bedecarratz Scholz
Abogado, Magíster y Doctor en Derecho
Director Observatorio de Ciberseguridad,
Universidad Autónoma de Chile

Minuta sumaria de exposición

Comisión de Futuro, Ciencias, Tecnología, Conocimiento e Innovación de la Cámara de Diputados, sesión del 21 de diciembre de 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)

I. Relevancia y urgencia del Proyecto

El Proyecto de Ley sobre Delitos Informáticos (en adelante el "Proyecto"), constituye un importante avance en materia de prevención y sanción de delitos informáticos. Su tramitación debe ser una prioridad legislativa para todas las partes, debido a los siguientes factores:

- Actualmente, los delitos informáticos son sancionados en Chile por la Ley N° 19.223, de junio de 1993, la que requiere una urgente actualización por razones por todos conocidas.
- Constituye un hecho público y notorio el incremento geométrico en número y potencialidad lesiva de delitos informáticos, tanto a privados como instituciones públicas, y que ponen en riesgo los intereses de privados y de la sociedad toda.
- También notable es el aumento del componente organizacional de la criminalidad informática, en virtud del cual esta clase de delitos son cometidos en una proporción cada vez mayor por organizaciones en vez de por individuos, lo que complejiza la persecución penal.
- Este tipo de criminalidad constituye una importante vía de financiamiento de Estados "parias" y organizaciones criminales, que es empleada para luego operacionalizar otro tipo de actividades delictivas.
- Finalmente, las características por todos conocidas de anonimato y comisión transnacional, implican un difícil esclarecimiento y persecución penal de los delitos informáticos.

Las anteriores características sustentan la necesidad urgente de aprobar el presente Proyecto, pero al mismo tiempo, de darle una correcta estructura y diseño. Ello supone efectuar un análisis de fondo desde el Derecho penal, manteniendo su naturaleza como norma sancionatoria de *ultima ratio* y evitando su desnaturalización.

II. Evaluación general del Proyecto y principales problemas detectados

En principio, el Proyecto de Ley constituye un importante avance en el cumplimiento de las obligaciones contraídas por Chile respecto del Convenio sobre la Delincuencia del 23 de noviembre del 2001 aprobado por Chile el 17 de noviembre de 2016 y actualmente vigente. Concretamente, las disposiciones que contiene son funcionalmente equivalentes a aquellas contenidas en el convenio, protegiendo similares bienes jurídicos, estableciendo verbos rectores de naturaleza comparable, y garantizando una adecuada persecución penal de las

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

conductas ilícitas. Sin embargo, el texto actual del Proyecto, en la versión que fue aprobada por la Comisión de Seguridad Ciudadana de la Cámara de Diputados, adolece de problemas de diseño que pueden implicar una difícil aplicación práctica, o bien una inadecuada protección de los bienes jurídicos en riesgo. Dichos problemas son los siguientes:

1. Dificultades probatorias: artículos 1°, 2° y 7°.
2. Vacío de punibilidad: art. 6°.
3. Eximente de responsabilidad indeterminada: art. 16 en relación con el art. 2°.

Estos problemas son expuestos de manera sucinta a continuación, junto a sugerencias y propuestas de mejora:

III. Dificultades probatorias

En primer lugar, es necesario hacer mención a las dificultades probatorias que puede originar la necesidad de acreditar un elemento subjetivo especial en ciertos delitos. Estos son el ataque de integridad sistema informático contemplado en el artículo 1°, el acceso ilícito contemplado en el artículo 2° y el fraude informático sancionado en el artículo 7°, que en su forma actual exigen que tales conductas sean realizadas de manera "deliberada e ilegítima".

Es necesario destacar, que el Convenio de Budapest, en su texto en inglés, exige que los delitos sean cometidos "intencionalmente" ("*intentionally*"), lo que fue traducido a su versión en español por "deliberadamente". Sin embargo, en el Derecho Penal chileno, este elemento se entiende implícito en todos y cada uno de los delitos que establece el Código Penal que son cometidos dolosamente. A saber, el artículo 1° inciso 2° del Código Penal establece que "Las acciones u omisiones penadas por la ley se reputan siempre voluntarias, a no ser que conste lo contrario."

Por lo tanto, lo que se quiso decir con este concepto, ya es válido de modo general por el art. 1° in. 2° del ya citado Código Penal. Sin embargo, esta redundancia no es el mayor problema, pues la nueva redacción implica que estos delitos tienen que ser cometidos con un ánimo especial, de muy difícil prueba en sede penal. Se exige que el delito sea cometido con una intención interna adicional o intensificada, la que deberá ser acreditada por los organismos persecutores. Esto significará necesariamente una enorme dificultad para los órganos de persecución penal, qué tendrán la muy difícil tarea de acreditar un ánimo subjetivo que, como se sabe, solamente existe en la mente del delincuente.

Ello se ve agravado por el hecho, de que no existen elementos fácticos concretos que representen dicho elemento subjetivo especial: piénsese en el "deliberadamente" del ensañamiento en el homicidio calificado, que se acredita con los rastros de la mayor energía violenta recaída sobre el occiso. Esta posibilidad no existe en delitos informáticos, pues es difícil acreditar materialmente un acto "deliberado" que sobrepase la ejecución dolosa de las conductas respectivas. Es decir, se genera una imposibilidad probatoria, qué redunda en la ineficacia de la persecución de esta clase de delitos. Esto es lo que ocurre con el actual artículo 2° de la Ley N° 19.223 que sanciona el acceso ilícito sólo en cuanto se ha hecho con un ánimo especial.

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

Debido a lo anteriormente expuesto, se sugiere respetuosamente eliminar la voz "deliberada" en los artículos 1°, 2° y 7° del Proyecto.

IV. Vacíos de punibilidad

Un segundo problema detectado está relacionado con la versión actual del artículo 6° del Proyecto, que dice relación con la sanción de la receptación de datos personales. El objetivo original de esta norma era proteger la privacidad en general, es decir, evitar que datos informáticos que sean de propiedad de un tercero y que hayan sido obtenidos por vía ilícita, sean traficados entre personas que no tienen derecho a ello. La norma contempla una sanción penal similar a la prevista en el artículo 456 bis A del Código Penal respecto a la receptación de objetos robados, hurtados u objeto de abigeato, receptación o de apropiación indebida. Es del caso señalar, que el párrafo 202d) del Código Penal alemán contempla el delito de receptación de datos personales con un objetivo similar al que se ha propuesto al momento de proponer la norma original.

Sin embargo, en su tramitación ante la Comisión de Seguridad Ciudadana de la Cámara de Diputados, se restringió el objeto de protección de esta norma, enfocándola solamente en la Protección de Datos Personales según la Ley N° 19.628. Esto genera una desprotección manifiesta en cuanto a la receptación y el tráfico de datos privados no personales. Es decir, la receptación de datos personales y sensibles si estaría bajo sanción, pero cualquier otro tipo de datos que, pese a no ser personal, se encuentre bajo la propiedad de una persona o una organización, por ejemplo, información privada, creaciones del intelecto, propiedad intelectual, datos que constituyan información industrial, etc., no van a estar protegidos por esta norma. Esto es consecuencia de una desnaturalización del objeto original de esta disposición: la protección general de la privacidad de la información y que se restringió solamente a la de datos personales.

Derivado de lo anterior, el objeto de protección delineado en esta norma no pertenece a este campo normativo, sino a la protección de los datos personales. En específico, el Proyecto de Ley sobre la Protección de Datos Personales ya contempla normas penales para sancionar el tratamiento ilícito doloso de datos personales (y sensibles) de terceros. Luego, una figura agravada como la que se pretende incorporar en esta norma, no pertenece a esta ley, sino que más bien a la de Datos Personales, sea el proyecto de ley o derechamente la Ley N° 19.628 actual. Mantener la norma en su versión actual en el Proyecto de Delitos Informáticos, generará un grave vacío de punibilidad y una falta de armonía con las demás disposiciones de esta ley.

En consecuencia, se sugiere mantener el texto aprobado por el Senado , introduciendo la figura calificada como un inciso nuevo, o bien trasladándola derechamente al Proyecto de Ley de Datos Personales.

V. Indeterminación de eximente

La investigación de brechas o vulnerabilidades en sistemas informáticos es esencial para impedir que usuarios maliciosos las aprovechen para efectuar un ataque y lesionar los derechos de las personas. Más específicamente, la búsqueda de vulnerabilidades y

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

notificación coordinada de ellas, permite a los responsables de sistemas informáticos, proveedores de servicios, organismos públicos, etc. cerrar las brechas, blindar los sistemas y contribuir a un ecosistema digital más seguro. Por lo tanto y desde una perspectiva penal, esta actividad de investigación, desarrollada en un marco ético y socialmente aceptable, contribuyen a la seguridad de todos. Por razones de política criminal, esta actividad no debe ni puede ser punible, sino más bien resguardada ante la persecución penal. Ahora bien, estos resguardos ya existen en nuestra legislación actual, a saber:

- **a.** El art. 10 N° 10 del Código Penal establece como exención de responsabilidad penal el "ejercicio legítimo de un oficio". Esto significa, que el desarrollo de actividades propias de un oficio que, al mismo tiempo, podrían ser consideradas como delictivas, no son perseguibles penalmente. En términos prácticos, abogados no son perseguidos por desacato ante tribunales por cuestionar fallos, periodistas no son perseguidos por injurias o calumnias cuando lesionan el honor de una persona, y doctores no son acusados por lesiones cuando intervienen a una persona en un pabellón. 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 hecho en transgresión a principios éticos o en vulneración a los derechos de la víctima, jamás podrán justificar la conducta.
- **b.** La figura del acceso punible ya ha sido tipificada en el art. 2° como "tipo abierto", esto es, se contemplan como requisito adicional la "ilegitimidad" o "ilicitud" de la conducta, obligando al juez valorar desde un punto de vista material lo que está prohibido. Esta característica es de especial relevancia, pues permite al juez eximir de pena conductas que pueden parecer accesos sin autorización formal, pero que al mismo tiempo no sean ilícitos, por ser necesarios para prevenir los daños producto de un ataque a la integridad de un sistema, por ejemplo.
- **c.** El art. 71 Ñ lit. c) Ley N° 17.336 permite expresamente la investigación en sistemas informáticos de terceros, legitimando dicha conducta en materia de propiedad intelectual y, por lo tanto, también en otras áreas del derecho (si no se sanciona lo menos, tampoco se sanciona en lo más).

Por otra parte, el art. 16 del Proyecto busca resguardar los comportamientos positivos, es decir, la búsqueda y notificación de vulnerabilidades. Al efecto, el artículo implementa una solución de notificación coordinada: si una persona efectúa un acceso no autorizado con la intención de detectar vulnerabilidades, no estará expuesto ante la persecución penal, si notifica estas mismas seguridades al "responsable del sistema informático, si ello fuera posible, y en todo caso a la autoridad competente". Sin embargo, el art. 16 adolece de tres errores o "vicios" de naturaleza penal y además constitucional.

- **a.** Especificar el plazo de notificación de vulnerabilidad. En esta materia existe diversa normativa comparada e internacional, que disponen plazos de notificación de vulnerabilidades, con el fin de no dejar al arbitrio del sujeto activo la puesta en conocimiento de la vulnerabilidad al afectado. En este sentido, se sugiere revisar

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

ejemplos de naturaleza comparada o aquellos contenidos en cuerpos normativos del *soft law*, con el objeto de consensuar un plazo de reporte de vulnerabilidades adecuado.

b. Especificar el organismo que recibirá la notificación. El proyecto de ley establece que la "autoridad competente" recibirá la notificación de vulnerabilidad, pero no especifica qué organismo específico tendrá a su cargo dicha competencia. Además, es necesario hacer presente a la Comisión, qué otorgarle mayores atribuciones a organismos públicos constituye una atribución específica y privativa del Presidente de la República, en virtud del artículo 65 de la Constitución Política de la República de Chile. El actual art. 16 en comento tuvo su origen en una indicación parlamentaria. Al establecer nuevas atribuciones a un organismo público y, con ello, generar gastos, podría estar afecta un vicio de inconstitucionalidad debido a la citada norma.

c. Finalmente, es necesario especificar aspectos puntuales mínimos del reglamento, tales como la autoridad que lo expedirá, el plazo al efecto y demás requisitos mínimos y elementos que constituirán el andamiaje sobre el cual se construirán las disposiciones reglamentarias.

Si bien consideramos que el artículo 16 actual del Proyecto constituye un claro avance en relación con la versión aprobada por el Senado que, tal como ya lo hemos planteado en otra oportunidad, adolecía de diversas incoherencias y características que lo hacían ser contraproducente a los fines que la propia disposición tenía, no es menos cierto que se hace necesario especificar la norma, con el objeto de garantizar su efectividad y permitir una operacionalización adecuada de la investigación y reportes coordinados en materia de ciberseguridad.

¡Muchas gracias!

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