REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA
VOL. 7 NÚM. 2 (2018) • PÁGS. 1-3 • DOI 10.5354/0719-2584.2018.51992

EDITORIAL

Agenda legislativa sobre ciberseguridad en Chile

Daniel Álvarez Valenzuela

Editor, Revista Chilena de Derecho y Tecnología

En los últimos editoriales he descrito cómo la agenda pública regional se ha visto permeada por el creciente número de incidentes de ciberseguridad que han afectado a diversas organizaciones públicas y privadas, especialmente en el sector financiero y entre tratadores masivos de datos personales, que han sido objeto de intrusiones en sus redes o sistemas, han tenido pérdidas patrimoniales significativas o han visto filtradas sus bases de datos.

La reacción de los Estados y los gobiernos en la región ha sido dispar. Algunos han enfocado sus esfuerzos en contar con políticas o estrategias sobre ciberseguridad, mientras otros avanzan decididamente en implementar marcos normativos que intenten resolver los nuevos escenarios jurídicos que la ciberseguridad, en general, y la delincuencia informática, en particular, suponen para nuestra región, los derechos de las personas y la economía. Con todo, todavía existe un importante número de países que sigue sin dar estos primeros pasos.

En el caso de Chile, habiendo transcurrido ya casi dos años desde la aprobación de la Política Nacional de Ciberseguridad —que entre sus múltiples medidas contiene diversas iniciativas que requieren discusión legislativa—, el proceso de implementación ha comenzado a rendir sus primeros frutos, que revisaremos brevemente a continuación.

Primero, cabe destacar la moción parlamentaria de autoría de los senadores Kenneth Pugh, Pedro Araya, Carlos Bianchi, Álvaro Elizalde y Víctor Pérez, presentada en mayo de 2018, que propuso establecer el mes de octubre como el Mes Nacional de la Ciberseguridad, en consonancia con iniciativas similares desarrolladas hace varios años en Estados Unidos y en la Unión Europea. La moción fue rápidamente tramitada y obtuvo apoyos transversales que permitieron que se publicara en el *Diario Oficial* el pasado 1 de octubre bajo el número 21.113. La creación del Mes de la Ciberseguridad no solo representa un ejercicio simbólico de relevancia, sino que también facilita el desarrollo coordinado de actividades de concienciación en materia de seguridad digital, tanto desde el sector público como del privado, ayudando de esta manera a incrementar los niveles de madurez organizacional en Chile. De este modo, se cumplió cabalmente con la medida 17 de la Política Nacional de Ciberseguridad.

Segundo, haciéndose cargo de —quizás— una de las dimensiones más importantes de la ciberseguridad, desde el año 2017 se discute en el Congreso Nacional el proyecto de ley sobre datos personales (Boletines 11.144 y 11.092, refundidos) que incorpora la seguridad en el tratamiento de datos personales como un principio rector y como un deber de información y transparencia respecto a las políticas y medidas adoptadas por la organización. Asimismo, se establecen una serie de medidas y obligaciones que deberán adoptar e implementar los responsables y encargados de tratamientos de datos personales con el objeto de evitar la destrucción, filtración, pérdida o alteración de datos personales que administran. Para ello, el proyecto de ley establece la obligatoriedad de adoptar medidas de seguridad idóneas según el tipo de datos de que se trate y considerando factores como el análisis de riesgo, el estado de la técnica, entre otros. Se introducen, además, la obligación de reportar las brechas de seguridad que afecten datos personales, ya sea a la autoridad de control —función que asumirá el Consejo para la Transparencia— y, en ciertos casos, a los titulares de datos personales, junto con un estricto régimen sancionatorio en casos de incumplimiento de estas futuras obligaciones.

Finalmente, el Ejecutivo ingresó a fines de octubre el proyecto de ley sobre delitos informáticos (Boletín 12.192-25), que se discute en primer trámite constitucional en la Comisión de Seguridad Pública del Senado. En términos generales, el proyecto de ley cumple con los propósitos declarados. Por una parte, actualiza la legislación sobre delitos informáticos a los nuevos tipos de criminalidad informática que han surgido en las últimas décadas; y, por otra, implementa algunas de las obligaciones específicas del Convenio de Budapest sobre Cibercrimen que Chile suscribió en el año 2017, como parte de la Política Nacional de Ciberseguridad. Sin perjuicio de ello, hay observaciones generales y particulares que formular a la propuesta específica del Ejecutivo y, en particular, quisiera llamar la atención sobre dos eventuales inconstitucionalidades del texto propuesto.

La primera de ellas relativa a las disposiciones sobre retención de metadatos de comunicaciones privadas, las que en nuestra opinión podrían ser consideradas inconstitucionales por cuanto no cumplen con los estándares de especificidad y determinación que se les exige a las normas que interpreten o restrinjan derechos fundamentales. En este caso concreto, respecto de los derechos a la vida privada, a la protección de datos personales y a la inviolabilidad de las comunicaciones privadas, todos garantizados en los numerales 4.º y 5.º del artículo 19 de la Constitución.

La segunda de las inconstitucionalidades detectadas se refiere a la disposición que establece como agravante especial el uso de tecnologías de cifrado, la que en nuestra opinión es inconstitucional por cuanto constituye una restricción ilegítima de la garantía de no autoincriminación contenida en el literal f) del numeral 7.º del artículo 19 de la Constitución. Si una persona tiene derecho a guardar silencio, a no aportar antecedentes probatorios en el proceso penal, resulta razonable sostener que

tiene derecho a utilizar mecanismos de cifrado. Desde un punto de vista de políticas públicas, el cifrado ha demostrado ser una de las herramientas técnicas más efectiva para la protección de la ciberseguridad de las personas, cuestión que incluso es considerada expresamente por la Política Nacional de Ciberseguridad que «reconoce el valor de las tecnologías de cifrado, que permiten dotar de niveles de confidencialidad e integridad de la información sin precedentes en nuestra historia». Esperamos que el legislador tome nota de estas observaciones.

Con todo, hay que destacar el avance de la agenda legislativa nacional en materia de ciberseguridad, quedando pendientes los avances en materia de gobernanza pública de la ciberseguridad y la espinosa regulación de las infraestructuras críticas, ambos cuerpos legales imprescindibles en un Estado con pretensión digital como el nuestro.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).