REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 12 (2023) • e73399 • DOI 10.5354/0719-2584.2023.73399
PUBLICADO: 31/12/2023

EDITORIAL

Avances legislativos sobre ciberseguridad en Chile

Michelle Bordachar Benoit
Universidad de Chile

El 12 de diciembre de 2023, el Congreso Nacional de Chile aprobó de manera unánime en ambas cámaras el proyecto de ley marco sobre ciberseguridad, posicionando al país como el primero de América Latina y el Caribe que contará con una Agencia Nacional de Ciberseguridad y con un marco regulatorio de vanguardia en esta materia.

El proyecto establece un modelo de gobernanza de la ciberseguridad basado en la colaboración intersectorial y en la prevención y gestión de riesgos e incidentes. Para ello se crea la institucionalidad y la normativa necesaria para estructurar, regular y coordinar las acciones de ciberseguridad de los sujetos obligados; entregando a la Agencia el liderazgo en la ejecución de las disposiciones de la ley. La ley también entrega las definiciones y los principios que serán útiles para guiar su correcta aplicación e interpretación; y contiene diversas disposiciones que apuntan a la concienciación de las personas en materia de ciberseguridad.

En cuanto a su ámbito de aplicación, la ley busca regular a los prestadores de servicios esenciales y a aquellos que sean calificados como operadores de importancia vital conforme al procedimiento administrativo y a los criterios establecidos al efecto. Sin perjuicio de lo anterior, en la misma ley se califica como servicios esenciales a todos los organismos de la administración del Estado, al coordinador eléctrico nacional y a los servicios prestados bajo concesión de servicio público.

En lo referido a los protocolos y estándares de ciberseguridad, las instituciones obligadas deberán aplicar las medidas que sean necesarias para la prevención y la gestión de los riesgos asociados a la ciberseguridad. Esta obligación exige a lo menos la debida implementación de los protocolos y estándares dispuestos por la Agencia o por el regulador sectorial, según corresponda. En el caso de los operadores de importancia vital, estos deberán además cumplir con las obligaciones específicas señaladas para ellos. Por último, la ley obligará a notificar los incidentes de ciberseguridad mediante el procedimiento que se contempla al efecto siguiendo los estándares de la Unión Europea. Respecto a las infracciones, la Agencia podrá multar a los infractores, siguiendo un modelo sancionatorio diferenciado según el sujeto obligado y la gravedad de las infracciones.

En cuanto a la institucionalidad, además de crear la Agencia Nacional de Ciberseguridad y el Consejo Multisectorial sobre Ciberseguridad; la ley da existencia legal al Equipo Nacional de Respuesta a Incidentes Informáticos (CSIRT Nacional); al CSIRT de la Defensa Nacional; al Comité Interministerial sobre Ciberseguridad; y a la Red de Conectividad Segura del Estado, encargada de proveer servicios de interconexión y conectividad a Internet segura a los organismos de la Administración del Estado.

Para prevenir conflictos normativos y posibles duplicidades en la imposición de sanciones, el proyecto contempla normas destinadas a garantizarla debida coordinación entre la Agencia y los reguladores sectoriales además de una regla expresa para impedir que el infractor pueda ser sancionado dos o más veces por unos mismos hechos y fundamentos jurídicos.

Por último, la ley incorpora dos mecanismos para promover la notificación responsable de vulnerabilidades. El primero exime a los trabajadores de la Agencia de la obligación de denunciar a aquellas personas que notifiquen la existencia de vulnerabilidades, obligando a mantener en secreto los detalles de la notificación, incluida la identidad del informante. El segundo mecanismo consiste en la modificación de la Ley 21.459 sobre delitos informáticos para incluir una exención de responsabilidad penal por el delito de acceso ilícito. Esta exención aplica siempre que la persona que ha realizado el acceso notifique la vulnerabilidad encontrada al responsable del sistema, y cumpla además con los requisitos copulativos que contempla la norma.

Destacamos esta última iniciativa, pues tal como fuera señalado en un editorial anterior —en el que se hizo un llamado a no criminalizar la actividad de quienes colaboran con la detección de vulnerabilidades—, esta actividad es esencial porque, al estar compuestos por cientos de miles de líneas de código, los sistemas informáticos son por naturaleza inseguros, y son las notificaciones oportunas de vulnerabilidades las que permiten parcharlas antes de que sean explotadas por agentes maliciosos.

Las discusiones más recientes reconocen este rol crucial de los procesos de notificación responsable de vulnerabilidades informáticas. Muestra de ello es la recomendación realizada por el Parlamento Europeo y el Consejo de la Unión Europea a sus países miembros para adoptar medidas que faciliten la divulgación coordinada de las vulnerabilidades, llegando incluso a alentarlos a no actuar penalmente ni exigirles responsabilidad civil por sus actividades cuando se trate de investigadores de seguridad de la información.

Si nos vamos al contexto más amplio de la regulación del entorno digital, este hito legislativo viene a sumarse a la Ley 21.459, promulgada en junio del año pasado, para formar con ella parte importante de los pilares fundamentales de la seguridad de la información. Sin embargo, el más fundamental de ellos, representado por la ley de datos personales, permanece ausente y lejos de convertirse en ley a pesar de sus más de seis años de tramitación.

Si consideramos que, en esencia, el fin último de la ley es la protección de las personas, lo lógico sería poner la mayor de las urgencias a aquella destinada precisamente a proteger sus derechos frente al tratamiento de aquellos datos que proporcionamos para participar del entorno digital.

En este punto es importante precisar que los marcos normativos a los que hemos hecho referencia, si bien son complementarios, abordan aspectos distintos. Por ello la existencia de unos en ningún caso suple la falta de otros. En efecto, no todo incidente de ciberseguridad afecta datos personales (*v.gr.* el ataque a una matriz de agua); ni toda afectación a los datos personales está mediada por sistemas informáticos (*v.gr*. caso del Banco Santander), o por la ocurrencia de una acción tipificada como delito informático (*v.gr.* el tratamiento ilícito de datos personales obtenidos lícitamente).

Es urgente que el Congreso Nacional despache el proyecto de ley sobre datos personales (boletines 11.144 y 11.092, refundidos). Múltiples artículos publicados en esta revista dan cuenta de los fundamentos de esta necesidad, siendo quizás el más importante de ellos que la protección del derecho a la autodeterminación informativa es condición habilitante para el ejercicio de la mayoría de los otros derechos que pueden ser ejercidos en el entorno digital: la igualdad ante la ley; el respeto y protección a la vida privada; la inviolabilidad de las comunicaciones privadas; la libertad de conciencia; la protección de la salud; la libertad de expresión; y la libertad de trabajo, por nombrar solo algunos.

Si además consideramos que en paralelo se encuentran avanzando otras iniciativas legislativas que involucran directa o indirectamente el tratamiento de datos personales (proyectos de ley sobre neuroderechos, inteligencia artificial, genoma humano, etcétera), amenazando con mermar aún más su situación, la protección de los datos personales debe transformarse en una prioridad inexcusable.

Dada su naturaleza, las personas seguirán cometiendo errores que comprometan su ciberseguridad y la de los demás, del mismo modo que los sistemas informáticos continuarán siendo vulnerables y los delitos informáticos seguirán ocurriendo. Esta realidad es inevitable, y fue precisamente en atención de ello que la ley marco sobre ciberseguridad no sanciona el hecho de haber sido víctima de un ciberataque. Pero necesitamos una ley que sancione severamente el tratamiento ilícito de datos personales, para evitar que un incidente de ciberseguridad dónde estos se vean afectados pueda terminar siendo aprovechado por terceros en formas que perjudiquen aún más los derechos de las personas afectadas.

Sabemos que el proyecto de ley sobre datos personales tiene una alta complejidad técnica y que el transcurso del tiempo no hace más que dificultar su tramitación, sin embargo, son numerosos los profesionales expertos en la materia dispuestos a colaborar en el avance del debate legislativo.

En esta línea, queremos destacar el esfuerzo realizado por distintos miembros del antiguo Centro de Estudios en Derecho Informático, hoy Centro de Estudios en

Derecho, Tecnología y Sociedad (reflejo de nuestra convicción sobre la necesidad de una visión más holística y multidisciplinaria de estas materias) de la Facultad de Derecho de la Universidad de Chile, mediante su participación en las sesiones de distintas comisiones del Congreso y la elaboración de informes de análisis legislativo. Reiteramos nuestro compromiso a seguir contribuyendo al debate público, fieles al rol de nuestra institución.

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.

DIRECTOR

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.io).