Regulación de la ciberseguridad en Chile, un ordenamiento jurídico fragmentado

Andrés Pumarino[1]

En el actual contexto de las organizaciones en un entorno de transformación digital, se hace necesario enfrentar los nuevos desafíos que se imponen tanto en el sector público como privado, donde el uso de las tecnologías se transforma en un importante aliado para las organizaciones y también en una herramienta que permite aumentar su productividad.

Sin embargo, así como el uso de las Tecnologías de la Información es un gran instrumento, también se transforma en un factor de riesgos. En las organizaciones sólo algunas unidades asumen la tarea de control y protección, debiendo también la alta dirección estar al tanto de los diversos cambios que se están generando. Una tendencia que se repite es la modernización de los marcos regulatorios que impactan en el gobierno interno de las organizaciones y que obliga a identificar de forma clara cuáles son las tareas, obligaciones, objetivos que tienen que desarrollar dado el nuevo escenario que estamos viviendo.

El problema que actualmente enfrentamos en la regulación en ciberseguridad es la existencia de un sistema legal fragmentado, esto se refiere a un conjunto de leyes y regulaciones que están dispersas y desorganizadas en diferentes niveles de gobierno o áreas temáticas dentro de nuestro país. En este contexto nos encontramos ante la ausencia de una codificación o consolidación completa de todas las normas en un solo cuerpo legal o un regulador que consolide ámbitos de regulación en este contexto.

Las razones detrás de la fragmentación pueden variar y están influenciadas por diversos factores. Algunos de ellos que pueden contribuir a la fragmentación legal en ciberseguridad incluyen:

a) Nivel de reguladores con mayor o menor expertise en el cambio de la ciberseguridad. Actualmente vemos en nuestro país que el sector financiero bancario a través de la Comisión de Mercado Financiero tiene mayor experiencia en materia de seguridad de la

[1] Abogado, Universidad Adolfo Ibañez. Magíster en Gestión de Negocios, Universidad Adolfo Ibañez. Profesor Asistente Adjunto PUC, Escuela de Ingeniería. Socio de Legaltrust. Consejero del Observatorio de Derecho y Tecnología UDD.

información y regulación a través de las normas RAN o Recopilación Actualizada de Normas.

b) Por otra parte, tenemos la ausencia de legislación especializada en nuestro país pues solo con el tiempo, se han creado leyes especializadas para abordar temas de ciberseguridad como la nueva Ley de Delitos Informáticos (Ley Nº 21.459) que deroga la Ley 19.223. Estas leyes especializadas pueden no estar completamente integradas con el resto del sistema legal.

La existencia de la fragmentación legal puede tener algunas consecuencias negativas, en el sector de la ciberseguridad, algunas de las dificultades son; la complejidad técnica de la materia y el uso de un lenguaje de especialidad, la diversidad de áreas económicas que se pueden ver afectadas, el impacto para ciudadanos, empresas y organismos públicos que deben cumplir con una variedad de leyes y regulaciones, a veces contradictorias entre sí por no tener un sistema de coherencia normativa.

Para abordar la fragmentación legal en ciberseguridad, algunos países pueden intentar realizar reformas legales que armonicen y consoliden leyes relacionadas en cuerpos legales unificados. También puede promoverse una mayor cooperación y coordinación entre los distintos niveles de gobierno para mejorar la coherencia del sistema legal.

Para hacerse cargo de estas dificultades el proyecto de Ley Marco de Ciberseguridad de Infraestructura Crítica de la Información (Boletín Nº 14847-06), contempla varias facultades a la Agencia Nacional de Ciberseguridad que busca crearse a través de este proyecto de Ley.

En el artículo 5 del mencionado proyecto de Ley se propone que en el caso de los organismos de la Administración del Estado e instituciones privadas que presten servicios esenciales, el cumplimiento de estas obligaciones exige, al menos, la debida implementación de los protocolos y estándares establecidos por la Agencia Nacional de Ciberseguridad, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva, de ser el caso.

La Agencia Nacional de Ciberseguridad deberá establecer protocolos y estándares diferenciados según el tipo de organización de que se trate y su relación con la prestación de servicios calificados como esenciales, teniendo especialmente en consideración las características y

necesidades de las pequeñas y medianas empresas, tal como se definen en la ley N° 20.416, que fija normas especiales para las empresas de menor tamaño.

El proyecto de Ley contempla en su Artículo 8, la creación de la Agencia Nacional de Ciberseguridad. Se destacan en sus funciones el velar por la protección, promoción y respeto del derecho a la seguridad informática, coordinar y supervisar la acción de los organismos de la Administración del Estado en materia de ciberseguridad.

El proceso de transformación digital que estamos viviendo tanto en el sector público como privado imponen también nuevos marcos regulatorios ajustados al ecosistema digital de las organizaciones, muchas de nuestras normas responden a un entorno analógico del siglo XX y tienen que adecuarse para tener la suficiente coherencia para responder al contexto digital que estamos viviendo y evitar un ordenamiento fragmentado en ciberseguridad.