EL MERCURIO Legal

Versión para imprimir El Mercurio.com

Legal |
Opinión | Artículo 2 de 2

Algunas consideraciones del proyecto sobre Agencia Nacional de Ciberseguridad e Infraestructura Crítica de la Información

"...Debe analizarse a la luz de varias regulaciones tecnológicas que están discutiéndose a nivel nacional, como la relativa a la actualización a nuestro marco normativo sobre protección de datos personales y la recién publicada normativa sobre Fintech y Open Banking (...). Además, a nivel internacional el tema está avanzando con bastante rapidez, especialmente en cuanto a la regulación sobre IA en Europa..."

Miércoles, 30 de agosto de 2023 a las 9:18

Juan Pablo González

El proyecto que crea la Agencia Nacional de Ciberseguridad y protege la Infraestructura Crítica de la Información, denominado "Ley Marco de Ciberseguridad" (Boletín 14.847-06) —que ya se encuentra en su segundo trámite constitucional (Cámara de Diputados) y en el cual recientemente se cerró el plazo para la formulación de indicaciones—, tiene varios aspectos que son interesantes de tener en consideración desde una perspectiva de la regulación no solo para los órganos públicos sino especialmente para el mundo privado y, en particular, para aquellas instituciones que son críticas.

Un punto para tener en cuenta es que esta iniciativa, a través de la creación de la Agencia Nacional de Ciberseguridad, viene a coordinar una serie de regulaciones que actualmente se hacen cargo del asunto, especialmente en sectores que son críticos para el país, como telecomunicaciones, eléctrico, pensiones, casino y juegos y, finalmente, financiero. Este último, sin lugar a duda, ha sido un referente en cuanto a la obligación de la gestión de riesgos de seguridad de la información y ciberseguridad, especialmente por la dictación de normas específicas (RAN 20-10, por ejemplo) por parte de la Comisión para el Mercado Financiero (CMF).

Otro aspecto relevante es la denominación de servicios esenciales y aquellos que son operadores de

importancia vital, puesto que no solo órganos que conforman la Administración del Estado (por ejemplo, un hospital) pueden caer dentro de esta categoría, sino, especialmente, el sector privado en ciertas áreas estratégicas. El proyecto, en la versión aprobada en el primer trámite constitucional, tiende a usar ambas expresiones como sinónimos y se aleja de la denominación que usualmente es utilizada a nivel internacional para este tipo de organizaciones, conocidas usualmente como "infraestructuras críticas".

A mayor detalle, el artículo 2º señala que el servicio esencial es aquel "cuya afectación o interrupción tendrá un impacto perturbador en el normal funcionamiento de la defensa nacional, la sociedad o la economía", mientras que el operador de importancia vital es aquel que reúna una serie de requisitos, a saber: a) un operador que presta un servicio calificado como esencial, b) si dicho servicio depende de las redes y sistemas informáticos y c) que en el caso de que ocurra un incidente de ciberseguridad (como un ataque de secuestro de datos), este tendrá un impacto perturbador en la prestación de dicho servicio, lo que podría asociarse a un análisis de la potencialidad de usuarios afectados, por ejemplo, y, por ende, a la magnitud de dicho evento.

Este punto, que puede parecer irrelevante, no lo es, si se tienen en cuenta las obligaciones que establece el artículo 5º y 6º del proyecto, que van desde la identificación de los riesgos de ciberseguridad hasta la total implementación de un sistema de seguridad de la información, que incluye el nombramiento de un encargado de ciberseguridad (CISO) para aquellos servicios esenciales y operadores de importancia vital e, inclusive, el régimen de infracciones es diferenciado, siendo aquellas gravísimas de configuración para los operadores de importancia vital.

Sin lugar a duda, esta propuesta debe analizarse a la luz de varias regulaciones tecnológicas que están discutiéndose al día de hoy a nivel nacional, como es la relativa a la actualización a nuestro marco normativo sobre protección de datos personales y la recientemente publicada normativa sobre Fintech y Open Banking —ambas abordan de manera específica obligaciones de las organizaciones en cuanto a la gestión de los riesgos de seguridad de la información o de los datos personales, respectivamente—. Además, a nivel internacional el tema está avanzando con bastante rapidez, especialmente en cuanto a la regulación sobre Inteligencia Artificial en Europa, que tiene un enfoque de identificación, evaluación y mitigación de riesgos de los sistemas que soportan este tipo de tecnología.

Finalmente, considerando el set de indicaciones del Ejecutivo así como varias que han presentado los congresistas, y pronto a retomarse el debate legislativo, esperamos que se pueda aclarar tanto este tema como otros del citado proyecto, para lograr así un balance entre la oportuna mitigación de los riesgos de ciberseguridad y el resguardo de los derechos de las personas en el ciberespacio, con el legítimo interés de las organizaciones de tener un marco claro de regulación en la materia que les permitan adoptar acciones concretas, sin el riesgo de incurrir en multas por incumplimiento normativo.

** Juan Pablo González Gutiérrez es consejero externo del Observatorio Derecho y Tecnología de la Universidad del Desarrollo.*