

Chile: iluminando el camino de la Ciberseguridad en Latinoamérica y el Caribe

Diego Lisoni¹

Nuestro país en el corto plazo va a contar con uno de los marcos regulatorios más robustos en materia digital de toda Latinoamérica y el Caribe, luego de que entre en vigencia la Ley Marco de Ciberseguridad el próximo año 2025, la nueva Ley sobre Protección de Datos Personales inspirada en el Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) en dos años más y, junto con esta, eventualmente la ley que regula los sistemas de IA que actualmente se está debatiendo en el Congreso Nacional.

Luego de años de discusión legislativa, la luz al final del túnel regulatorio digital chileno comienza a asomarse y, desde el año 2025, se espera que cada vez esté más cerca cuando, asimismo, exista mayor claridad respecto a la normativa secundaria que aplicará en materia de protección de datos personales y ciberseguridad, dictada tanto por SEGPRES y el Ministerio del Interior (Coordinación Nacional de Ciberseguridad) en una primera etapa, así como más adelante por las futuras Agencia Nacional de Protección de Datos Personales y la Agencia Nacional de Ciberseguridad, respectivamente.

Con todo, en materia de ciberseguridad, a diferencia de lo que podría anticiparse en materia de protección de datos personales, el camino que podría recorrer Chile y, eventualmente, inspirar a toda la región, no se encuentra orientado específica ni necesariamente por un estándar de “oro” como lo es el RGPD de la UE, consolidado gracias a todas las opiniones y recomendaciones de la European Data Protection Board (EDPB), así como la jurisprudencia judicial y administrativa de las autoridades de protección de datos europeas.

Efectivamente, en materia de ciberseguridad podríamos identificar una serie de estándares fragmentados locales y en desarrollo desde hace varios años a nivel de la UE y Estados Unidos de América (USA), en la que la Ley Marco de Ciberseguridad en Chile emerge como una tercera vía para regular esta materia a nivel regional, mientras navegan al mismo tiempo a nivel internacional un contexto regulatorio altamente técnico y especializado (Ej. Normas ISO, NIST, etc.).

Por ejemplo, en USA recién se está en proceso de reglamentación e implementación de la “*Cyber Incident Reporting for Critical Infrastructure Act of 2022*” (CIRCIA), cuyo reglamento estuvo en Consulta Pública este año y que, en términos generales, establece el deber de determinadas entidades de reportar a la Cybersecurity & Infrastructure Security Agency (CISA) incidentes cubiertos en un plazo

¹ Investigador y Asesor en Políticas Públicas en Magliona Abogados. Ayudante en la Facultad de Derecho de la Universidad de Chile de los profesores Luis Cordero Vega, Natalia Muñoz y Claudio Magliona. Co-coordinador del Grupo de Trabajo de la Juventud de Internet Society Capítulo Chile (ISOC Chile).

de 72 horas a partir del momento en que la entidad crea razonablemente que se ha producido el incidente, así como en un plazo de 24 horas el pago de rescates como consecuencia de un ataque de ransomware.

Por su lado, en la UE se encuentra en proceso de implementación de la Directiva 2022/2555 “*on measures for a high common level of cybersecurity across the Union of 2022*” (NIS 2 Directive), que los países miembros debían transponer a leyes locales a más tardar este 17 de octubre de 2024, y que también establece obligaciones de reporte bajo un esquema que comienza con una alerta temprana a las 24 hrs del incidente. A mayor abundamiento, justamente el 17 de octubre la Comisión Europea publicó el texto del reglamento de implementación de la NIS 2 Directive sobre los requisitos técnicos y metodológicos de las medidas de gestión de riesgos de ciberseguridad para entidades y redes críticas (Ej. DNS; Cloud; Social Networks; etc.).

Ante este escenario fragmentado de la regulación mundial de la ciberseguridad (y de la gobernanza en general de internet), Chile emerge como un nuevo faro con la Ley Marco de Ciberseguridad, y la primera Agencia Nacional de Ciberseguridad en toda la región. Ya en otros países de LATAM (ej. Ecuador) la Ley Marco ha sido tomada en cuenta para nutrir sus propios debates legislativos y regulatorios.

En tal sentido, en la futura Agencia Nacional de Ciberseguridad recae una de las más grandes responsabilidades internacionales de la última década, para que tanto la regulación local en Chile y, eventualmente, la de toda la región, puedan conversar armoniosamente con los demás estándares internacionales que se encuentran en desarrollo a nivel mundial, promoviendo una coherencia e interoperabilidad normativa que fomente y no desincentive la exportación o importación de servicios y productos desde Chile y hacia el mundo para, en suma, seguir consolidando a Chile como Hub Digital en el Mercado Digital Regional.