

EDITORIAL

## Ciberseguridad en América Latina y ciberdefensa en Chile

Daniel Álvarez Valenzuela

*Editor, Revista Chilena de Derecho y Tecnología*

Tal como anticipamos en el editorial anterior, en América Latina y el Caribe crecientemente la ciberseguridad y la ciberdefensa han ido ocupando un espacio cada vez más relevante en la discusión pública y en la agenda regulatoria de los Estados que intentan ofrecer una respuesta política a un fenómeno que hace mucho tiempo dejó de ser únicamente preocupación de técnicos o ingenieros.

En la región es posible destacar que ya son diez los países que cuentan con una política o estrategia nacional de ciberseguridad. Recientemente se sumaron República Dominicana y Guatemala al listado integrado por Colombia, Trinidad y Tobago, Jamaica, Panamá, Chile, Costa Rica, México y Paraguay. Cabe destacar que varias de estas iniciativas de políticas públicas han contado con el apoyo decidido de la Organización de Estados Americanos a través del Programa de Seguridad Cibernética del Comité Interamericano contra el Terrorismo.

Este avance ha sido parcialmente reconocido en el recientemente publicado National Cyber Security Index (<https://ncsi.ega.ee/>) elaborado por la prestigiosa e-Governance Academy Foundation de Estonia y que mide el nivel de preparación de los países para prevenir amenazas a la ciberseguridad y la gestión de incidentes cibernéticos. En América Latina y el Caribe son analizados once países y lideran el ranking Panamá, Colombia y Chile, y se identifican dos áreas que han recibido nula o escasa atención por parte de los estados: la protección de servicios esenciales (incluyendo infraestructura crítica) y las ciberoperaciones militares.

En el caso de Chile, una de las medidas sectoriales contenidas en la Política Nacional de Ciberseguridad consistía precisamente en el establecimiento de una Política de Ciberdefensa que fijara los objetivos a ser cumplidos gradualmente hasta el año 2022 por las instituciones de la Defensa Nacional.

La Política de Ciberdefensa es el resultado del trabajo iniciado en el año 2015, y que comprendió la realización de diversos talleres temáticos, en los que participaron representantes de las instituciones de las Fuerzas Armadas, de organizaciones académicas, de la sociedad civil organizada, de otras reparticiones de gobierno, además de especialistas convocados al efecto.

El texto de la Política de Ciberdefensa está estructurado en seis secciones, que comienzan con una introducción y un diagnóstico a los nuevos riesgos y amenazas que supone el ciberespacio para la defensa nacional. Luego, se presenta la propuesta de aplicación de los principios de la Política de la Defensa Nacional al ciberespacio, y una propuesta de políticas, entre las cuales se consideran aspectos como el empleo de los medios de ciberdefensa, la cooperación internacional, el desarrollo de capacidades de ciberdefensa y, finalmente, se identifican los instrumentos de la política y las responsabilidades de implementación.

En términos políticos, el documento configura la respuesta del Estado de Chile a los nuevos riesgos y amenazas que el ciberespacio genera para las capacidades de la defensa nacional, las cuales incluyen, entre otros elementos, la información, infraestructura y operaciones de defensa.

La Política de Ciberdefensa se sustenta formalmente en la Política de Defensa del Estado de Chile y, por tanto, sostiene los mismos principios básicos que tienen plena expresión en el ciberespacio: el respeto del derecho internacional público, incluyendo la abstención del uso y la amenaza del uso de la fuerza, la legítima defensa, y el respeto a la soberanía; la promoción de la democracia y el respeto a los derechos humanos; y la protección de la población, de los intereses nacionales y de la integridad territorial.

En el plano internacional y regional, la Política de Ciberdefensa constituye un esfuerzo por promover la implementación de medidas de transparencia y generación de confianzas en el sector de la defensa en la región, que son imprescindibles para la mantención de la paz y la seguridad en América Latina.

El desafío ahora, y tal como señalábamos en el número anterior, es implementar los instrumentos de política pública sobre ciberseguridad y ciberespacio que seguramente requerirán de cambios a la legislación relativa al ciberespacio, el que, como ya todos sabemos, no se encuentra en estado de naturaleza; al contrario, tanto su infraestructura física, la capa lógica y la faz de las interacciones humanas que ahí se producen, están plenamente reguladas por el derecho nacional de los países y el derecho internacional.

De ahí el desafío de profundizar la reflexión académica en las disciplinas temáticas cubiertas por la *Revista Chilena de Derecho y Tecnología*.