CAMARA CHILENA DE INFRAESTRUCTURA DIGITAL.

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 16.	Esa "libertad que tienen los proveedores de redes y servicios de usar las tecnologías para la prestación de todos los servicios sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos". Ese objetivo también debe ser protegido en materia de Ciberseguridad. No se ve reflejado en este punto de Supervisión de seguridad. Puede estar en riesgo los principios de neutralidad tecnológica y de neutralidad de la red y el objetivo de la seguridad de las redes y de la infraestructura? En el Parlamento se discute si es necesario o no actualizar la ley de neutralidad de red y permitir la gestión del tráfico, sin ese marco, la normativa estaría afectando los principios de no discriminación de la red.
Artículo 5.	Chile: Ciberseguridad y neutralidad tecnológica La transformación digital debe ser SEGURA. El incremento en el foco de ciberseguridad y protección de infraestructuras críticas es parte de los aspectos habilitantes de cualquier ecosistema digital. El Foro Económico Mundial (WEF) en su informe anual sobre los mayores riesgos a los que se enfrenta la humanidad, indica en el primer lugar al cambio climático, y en el segundo lugar están los ciberataques y la crisis del agua. Chile, durante la administración de la Presidenta Bachelet, publicó la política en materia de ciberseguridad, con una mirada que apunta al año 2023, para "alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente, que orienta la acción del país en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios

	del ciberespacio". Junto con los desafíos de ciberseguridad, éstos deben estar acompañados con el principio de "neutralidad tecnológica", asunto que nuestro país ha seguido invariablemente, permitiendo que los concesionarios confluyan en diversas y distintas tecnologías, en tanto, mantengan la provisión del servicio concesionado. las letras k) determinaciones nacionales e internacionales en relación a los riesgos de seguridad asociados al uso de determinados equipos o proveedores; y la letra l) integridad de la cadena de suministros de equipos y software; se alejan de los principios de neutralidad tecnológica y no discriminatoria. Esto se aleja de la tradición regulatoria del regulador.
Comentarios Generales.	Es una preocupación que la masificación en el uso de tecnologías de información y comunicaciones (TIC), junto con servir al desarrollo del país, conlleva riesgos de espionaje, sabotaje, fraudes o ciberataquesques, que pueden afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile. Aquí es donde el Estado no puede tentarse por vetos, ni por soluciones parciales, sesgadas y restrictivas. No puede abanderarse discriminatoriamente por razones políticas sobre respuestas técnicas y soluciones tecnológicas. En medio de esta tensión geotecnológica, Chile podría tener la tentación de romper con su tradición y tomar posición por uno de los bandos en cuestión. Sería un error y de un impacto irreversible. Mientras un par de países promueven el veto, el bloqueo, la restricción y la hegemonía tecnológica, nuestro país debe ser el referente de la neutralidad tecnológica, la igualdad de concurrencia de operadores, fabricantes, integradores, proveedores, agregadores, resguardando siempre que

	es el usuario quien se beneficia de esa oferta y competencia. El regulador debe aportar con su experiencia a la política nacional de ciberseguridad, donde además concurren otros actores públicos y privados ,y ajustar toda nueva normativa técnica sobre la visión común que define el tipo de desarrollo digital que le ofrecemos a los ciudadanos. Uno de esos garantes acuñados y promovidos han sido los principios de neutralidad tecnológica y de no discriminación que ha sido un sello de la regulación sectorial por años, así como también la jurisprudencia derivada de los órganos de competencia y por los tribunales del país. Los resguardos y los objetivos de ciberseguridad no pueden ser opuestos a garantizar la competencia y neutralidad. Una buena normativa en materia de la gestión de los riesgos de seguridad, no puede estar asociada a la restricción, discriminación y arbitrariedad a priori y por defecto de un uso determinado de ciertos equipos o proveedores. Una normativa no debe favorecer ni perjudicar a ninguna tecnología, dado que es el mercado y los consumidores quienes tienen el poder de elegir. El mundo de las telecomunicaciones cambió. Sigue y seguirá cambiando. La conversación dejó de ser cerrada, propia de algunos conspiscuos actores y revestida con un rebuscado lenguaje técnico de difícil comprensión por parte de la mayoría de la población. Ya nada es puertas adentro, sino que la actuación es global y donde concurren una amplia cartera de proveedores, convirtiendo a este sector en el más competitivo del mercado. Chile tiene la oportunidad de crear una gobernanza en ciberseguridad para la era digital, mejorar las

	capacidades técnicas, ajustar los marcos regulatorios y construir un arquitectura legislativa que promueva la participación de manera satisfactoria para todos los actores, sin importar origen y condición, ni importar prejuicios que nos alejan de nuestra tradición regulatoria en telecomunicaciones.