JJR Abogados Limitada

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
Artículo 1.	Consagración de los principios de neutralidad tecnológica y no discriminación. La industria y regulación en telecomunicaciones tiene una larga tradición de respeto a los principios de neutralidad tecnológica y no discriminación, lo que se ha manifestado en la normativa y jurisprudencia relacionada a dicha industria. En consecuencia y dado que estamos en presencia de una primera norma técnica referida exclusivamente a la temática de ciberseguridad en telecomunicaciones, consideramos pertinente incluir una redacción que consagre los mencionados principios, a fin de que sean éstos quienes informen la totalidad del texto y que no exista ninguna disposición o artículo que pueda ir en contra de ellos. Hemos visto que la administración pública utiliza esta técnica normativa (Ley 19.880, que establece las Bases del Procedimiento Administrativo que Rigen los actos de los Órganos de la Administración del Estado y Ley N° 21.180, de Transformación Digital del Estado), lo que favorece su inclusión para una mejor interpretación en su conjunto. En el documento denominado "Resumen y Fundamentos del Tema de la Consulta", se señala que "la normativa sectorial de telecomunicaciones contempla relativamente pocas disposiciones orientadas de forma clara a prevenir, mitigar y remover riesgos que son consustanciales al diseño, instalación y operación de las redes y sistemas de telecomunicaciones contemporáneos. Considerando lo expuesto en el contexto dado por la Política Nacional de Ciberseguridad, la Subsecretaría de Telecomunicaciones ha decidido establecer una normativa para el sector que

	la ley coloca bajo su esfera de atribuciones y que aborde esa materia de forma específica. El objetivo de esta regulación consiste en constituir un marco que contribuya a proteger a los usuarios de servicios de telecomunicaciones mediante mejoras a los estándares con que son diseñadas, implementadas y operadas las redes empleadas para su prestación". Dado que el objetivo explícito de esta normativa es la creación de un marco general que entregue protección a los usuarios, se sugiere agregar un inciso al Artículo 1° de la Norma Técnica con la siguiente redacción: "Para la consecución de los mencionados objetos, la presente norma técnica se guiará por la aplicación estricta de los principios de neutralidad tecnológica y no discriminación, razón por la cual ninguna tecnología, ningún proveedor ni ningún equipo, independiente del país de origen, será favorecida o perjudicada, siendo los operadores relevantes o los usuarios finales, libres de elegir aquella tecnología, proveedor o equipo que mejor se adecue a sus necesidades".
Artículo 5.	La Propuesta Normativa viola el principio de neutralidad tecnológica. El borrador de norma técnica, en el mencionado artículo 5° letras k) y l), rompe con años de tradición normativa de respeto al principio de neutralidad tecnológica (un ejemplo reciente es la Ley 21.180 que modificó la Ley 19.880 de procedimiento administrativo, en cuanto incluyó, entre otros, una regulación específica para la

	tramitación electrónica de tales procedimientos. En su artículo 16 bis, se consagra el principio de neutralidad tecnológica, el cual consiste en que los individuos y organizaciones tengan libertad de elegir la tecnología más adecuada para sus fines. https://www.leychile.cl/Navegar?idNorma=210676&idVersion=Diferido). Subtel ha sido el principal y permanente impulsor y defensor de dicho principio, el cual sólo ratifica que la regulación no debe favorecer ni perjudicar a ninguna tecnología, dado que es el mercado y los consumidores quienes tienen el poder de elegir aquella que mejor satisfaga sus necesidades. La inclusión del concepto de "integridad de la cadena de suministros" en el artículo 5 Letra l) de la Propuesta Normativa, implica el establecimiento de un elemento subjetivo y arbitrario acerca de lo que se entiende por ciberseguridad, que nada tiene que ver con los objetivos planteados en el documento que fundamenta la presente consulta pública. En efecto, es de conocimiento público las disputas tecnológicas que hoy está enfrentando a Estados Unidos con China, en la que el primero de dichos países ha impuesto, por una parte, sendos vetos a la comercialización de equipos y tecnología de origen chino y, por la otra, ha prohibido la venta, embarques y entrega de semiconductores de fabricación estadounidense (tales como Qualcomm) a cualquier empresa de origen chino (https://www.cnbc.com/2020/05/15/us-china-tensions-rise-as-trump-administration-moves-to-cut-huawei-off-from-global-chip-suppliers.html). Sabemos que los semiconductores cumplen una labor fundamental en la fabricación de dispositivos móviles y redes de telecomunicaciones, lo que, eventualmente, puede traer consecuencias a las empresas chinas que participan de ese mercado y, adicionalmente, dañará de manera directa e indirecta el desarrollo de la industria de las telecomunicaciones en Chile.

Artículo 6.	Continuación artículo 5… En razón de lo anterior y haciendo una interpretación conservadora de lo dispuesto en la letra l) del artículo 5° del borrador de norma técnica, se entendería que, por ejemplo, un fabricante de origen chino tendrían problemas en la elaboración de sus productos, toda vez que, supuestamente, sus respectivas cadenas de suministro se verían afectadas por el hecho de no contar con los semiconductores que han utilizado históricamente hasta antes de la prohibición establecida por el gobierno de los Estados Unidos. Esta conclusión traería como consecuencia que los proveedores de dicho país se encontrarían vetados, ahora por el Gobierno de Chile, de participar en la industria de las telecomunicaciones y de prestar servicios a los operadores relevantes de este sector económico. Ello por cuanto tales operadores estarán obligados, según el mencionado artículo 5 inciso segundo letra l), a "garantizar un nivel adecuado de seguridad de las redes y sistemas, tomando en consideración la naturaleza y el contexto de servicios prestados, los riesgos asociados y la tecnología disponible, así como tener en cuenta, a lo menos, los siguientes conceptos: … l) integridad de la cadena de suministros de equipos y software;". Por lo tanto, si un fabricante llegase a tener inconvenientes con la integridad de la cadena de suministros, por el hecho que el gobierno de Estados Unidos no permite a los fabricantes globales de chipsets venderle su producción, quiere decir que dichas empresas representarían un riesgo para las redes y sistemas utilizados en la prestación de servicios de telecomunicaciones.
Artículo 7.	Continuación artículo 5… Según el diccionario de la Real Academia Española de la Lengua, el vocablo "integridad" significa "cualidad de

	íntegro". Por su parte, la palabra "íntegro", según la misma fuente, significa "1.- Que no carece de ninguna de sus partes" o "2.- Dicho de una persona: recta, proba, intachable". En consecuencia, si las redes fabricadas por un proveedor de origen chino carecen de semiconductores o éstos no detentan cualidades mínimas de seguridad o calidad, se podría interpretar como un incumplimiento a la norma técnica que nos ocupa, con el consiguiente perjuicio a los operadores, a los consumidores y al ecosistema en su conjunto. Esta situación resulta inaceptable desde todo punto de vista, más aún en momentos en que Chile y el mundo entero han tomado conciencia de la importancia de contar con internet de alta calidad y velocidad. De mantenerse la prohibición impuesta por Estados Unidos a la comercialización de semiconductores para fabricantes chinos, se podría cuestionar que los productos de dichos fabricantes no cumplen con la integridad de la cadena de suministro, lo que atenta directamente con el principio de neutralidad tecnológica. Por su parte, el Tribunal de Defensa de la Libre Competencia (https://www.tdlc.cl/nuevo_tdlc/wp-content/uploads/Recomendacion_Normativa/Proposicion_14_2014.pdf https://www.tdlc.cl/nuevo_tdlc/wp-content/uploads/sentencias/Sentencia_45_2006.pdf) ha sido férreo defensor de dicho principio, ya que entiende que es la manera de desarrollar la industria y de mejorar el servicio a los consumidores. Todas las sentencias dictadas por el TLC (que han sido ratificadas por la Corte Suprema) en el ámbito de las telecomunicaciones, han sido drásticas en fijar los principios de neutralidad tecnológica y no discriminación como rectores de la política de telecomunicaciones en el país. De mantenerse en el borrador las cláusulas relativas a los "riesgos de seguridad asociados al uso de determinados equipos o proveedores" y a la "integridad de la cadena de

	suministros de equipos y software", estaríamos dejando el desarrollo tecnológico a merced de la interpretación subjetiva del regulador de turno, pudiendo constituir una conducta discriminatoria en contra de algunas empresas que supuestamente caerían en la configuración de tales riesgos. El fundamento de lo anterior se basa en la total y absoluta inexistencia de razones de tipo técnico o económico que justifiquen la imposición de este tipo de sanciones o la configuración de estas conductas a un determinado fabricante.
Artículo 8.	Continuación artículo 5… El borrador reducirá la competencia en la industria El borrador de norma técnica que nos ocupa tiene serios problemas de libre competencia, dado que podría impedir la participación de algunas empresas en el mercado relevante de la fabricación de redes y tecnología, lo que resulta completamente anticompetitivo, injusto e improcedente. Como se ha señalado, no existen razones económicas ni técnicas para establecer una limitación en ese sentido. En consecuencia, la competencia en esta industria se vería severamente afectada por esta norma técnica, en caso que se mantengan las cláusulas ya señaladas. Junto con ello, se producirán desincentivos a la inversión para las empresas que se encuentren potencialmente vinculadas con los riesgos que señala la norma técnica, situación que también afectaría a la libre competencia en nuestro país. Adicionalmente, esta limitación o restricción de

	participar de dichas compañías, tendrá un costo económico muy alto para los operadores de telecomunicaciones, toda vez que no podrán optar a mejores precios, más proveedores y, peor aún, se verían amenazados de tener que reemplazar la infraestructura actualmente desplegada. Como es sabido, la existencia de menor competencia en este mercado traerá como consecuencia lógica una inversión significativamente menor en investigación y desarrollo, lo que afectará directamente el desarrollo de nuevas tecnologías y la reducción de las brechas digitales. La secuencia es conocida y fácil de entender: cuando hay menos actores en el mercado, habrá una menor voluntad de invertir y, como corolario, menos competencia y un menor desarrollo tecnológico. Sin duda alguna, ello repercutirá en los niveles de ciberseguridad de las redes de telecomunicaciones, lo que constituiría un contrasentido de la norma técnica sometida a consulta pública, dado que es precisamente lo que se quiere evitar. En definitiva, una discriminación como la que se propone iría en contra de las normas de libre competencia y no sería aceptada por ningún tribunal de este país, amén de no favorecer la libre entrada de las tecnologías de punta que se requieren cada vez más en nuestro país. De aplicarse los artículos ya mencionados, el mercado en esta industria vería reducido el número de actores de manera importante, con las consiguientes repercusiones en la calidad de servicio al cliente y en el desarrollo tecnológico.
Artículo 9.	Continuación artículo 5… El borrador dañará severamente el desarrollo de los

	operadores de telecomunicaciones y coartará su capacidad de elección. Esto ocurrirá por el hecho que los operadores no tendrán la posibilidad de elegir al proveedor o fabricante que deseen o que necesiten, limitando fuertemente su capacidad de elección, al crear artificialmente un monopolio o duopolio en la fabricación de redes y dispositivos, lo que reduce de manera importante la oferta en este mercado. La competencia mundial en esta industria se encuentra dominada por un número reducido de actores, habiendo competencia entre ellos en la mayoría de los países. Los clientes de tales actores son, principalmente, las operadoras de telecomunicaciones, quienes despliegan redes y comercializan dispositivos móviles, lo que hace posible la comunicación y el acceso a internet de la mayoría de los chilenos. Si tales operadores ven sustancialmente reducidas sus opciones, la consecuencia inmediata es un daño irremediable en sus respectivos desarrollos. Igual gravedad reviste el hecho que, de prosperar la normativa tal cual está en el borrador sometido a consulta pública, los operadores verán afectadas las redes que se encuentran actualmente desplegadas, ya que, dependiendo de "los riesgos de seguridad asociados al uso de determinados equipos o proveedores" y de la "integridad de su cadena de suministro", se podrían ver obligados a reemplazar total o parcialmente sus redes y sistemas "riesgosos". Lo anterior provocaría un enorme impacto negativo y produciría grandes pérdidas económicas tanto a los operadores como a los consumidores, además de generar problemas relacionados a las obligaciones de infraestructura crítica reguladas en la Ley N°20.478, sobre Recuperación y Continuidad en Condiciones Críticas y de Emergencia del Sistema Público de

	Telecomunicaciones y el Decreto N°60 del año 2012, del Ministerio de Transportes y Telecomunicaciones, que establece el Reglamento para la Interoperación y Difusión de la Mensajería de Alerta, Declaración y Resguardo de la Infraestructura Crítica de Telecomunicaciones e Información Sobre Fallas Significativas en los Sistemas de Telecomunicaciones.
Artículo 10.	Continuación artículo 5… El borrador podría implicar que ni los operadores de telecomunicaciones ni los consumidores obtengan prontamente los beneficios que trae el 5G. Desde hace ya dos años que Subtel ha sido uno de los principales impulsores de la implementación de la tecnología 5G en nuestro país. Como sabemos, 5G será un hito en el desarrollo de la industria de las telecomunicaciones pero, además, impactará de manera relevante en el desarrollo de los procesos productivos de muchas otras industrias y del consumidor final. Esta tecnología permitirá a los ciudadanos tener acceso real a una mejor educación, mejor salud, mejores negocios y mejor trabajo. Sin embargo, al limitar la capacidad de las redes y, por ende, de internet, dichos beneficios no alcanzarán a todos aquellos que lo necesitan. Sin ir más lejos, una de las principales conclusiones obtenidas de lo que está ocurriendo con la actual pandemia, se relaciona con el aumento significativo y exponencial en el tráfico de datos, por lo cual necesitaremos con urgencia una red robusta, con la mejor solución tecnológica y la mejor conexión posible.

	De lo contrario, seguiremos con la misma educación, salud y calidad de trabajo. La expansión actual del coronavirus cambiará de manera definitiva la forma en que nos relacionamos, trabajamos y estudiamos, por lo que tener la posibilidad de contar con la mejor tecnología y las mejores redes se transforma en un imperativo para cualquier gobierno. De lo contrario, corremos seriamente el riesgo de un incremento significativo en el número de reclamos hacia los operadores, la industria en su conjunto y, lo que es peor, serán los consumidores quienes sufrirán los efectos de estas políticas públicas.
Artículo 11.	Continuación artículo 5… La ciberseguridad es un asunto eminentemente técnico, no político. Con el desarrollo y masificación de internet, el consumo creciente de datos a nivel mundial, la utilización de dicha plataforma para la generación de negocios y la progresiva migración de la economía tradicional a una economía digital, se ha generado paralelamente, una industria enfocada en la realización de fraudes y ataques a las redes y sistemas informáticos. Una de las particularidades de este fenómeno se relaciona con la falta de incidencia del factor territorial de estas acciones, debido a que se realizan a través de internet, lo que implica que puedan se ejecutar delitos desde y hacia cualquier lugar del mundo. En virtud de ello, tanto empresas como gobiernos (especialmente de países desarrollados) se han hecho cargo del fenómeno de la ciberseguridad, como una manera de proteger sus activos, sus negocios y sus clientes, además de haberse transformado cada día más en un asunto de seguridad nacional.

	Sin embargo y a pesar de las diversas motivaciones que puedan tener quienes realizan ataques o fraudes informáticos, la seguridad de las redes y sistemas sobre las cuales se ejecutan tales delitos, es un asunto esencialmente técnico, que se enfrenta de manera técnica y se supera igualmente con soluciones de carácter técnico. En ese sentido, nada tienen que ver las intenciones políticas de un país o bloque de países a favor o en contra de otras naciones. Si una empresa tiene problemas de ciberseguridad en sus sistemas, no se arreglará con un acuerdo político, sino que tendrá que convocar a empresas especializadas en solucionar tales inconvenientes y, además, en prevenir de los riesgos que puedan provocarse en el futuro. La experiencia sigue demostrando que esa es la manera de enfrentar las dificultades de ciberseguridad. Existe una creciente industria global de empresas que se dedican a resolver tales dificultades, a instalar soluciones para cada cliente, a prevenir de los riesgos y a capacitar a los trabajadores. Este es el foco de las medidas que toma el sujeto pasivo de los ataques relativos a ciberseguridad. Adicionalmente y a pesar de las afirmaciones y opiniones que pueda entregar un país determinado, no existe fundamento técnico alguno que habilite poner en duda la integridad de la cadena de suministros en la industria de las telecomunicaciones, por lo que tampoco hay razones que justifiquen la inclusión de los mencionados artículos en el borrador que nos ocupa. Asimismo, tampoco existen riesgos de seguridad asociados al uso de determinados equipos y proveedores, ya que es el mercado y los operadores quienes toman esa decisión, no arriesgándose a utilizar equipos no aptos o poco seguros para la prestación de los respectivos servicios. Los riesgos técnicos no pasan por el lugar de origen de las redes o de los dispositivos móviles, puesto que se generan con insumos de diversas partes del mundo. Ninguno de los fabricantes actuales puede trabajar “puertas adentro”, sino que

	actúan de manera global y se nutren de proveedores globales, puesto que, de lo contrario, no serían competitivos en dicho mercado.
Artículo 12.	Continuación artículo 5… Creemos que, para construir una normativa robusta en esta materia, resulta de mayor necesidad conocer la regulación de los países desarrollados en la materia, que han tomado medidas neutrales en ciberseguridad basados en consideraciones técnicas, sin ninguna limitación, restricción o discriminación de carácter político. Dado que hoy en Chile no existen dichas limitaciones para ninguna tecnología ni proveedor en particular, consideramos que lo dispuesto en el artículo 5° inciso segundo letras k) y l) no constituyen un avance en la regulación, sino que, por el contrario, llevará a confusiones y malinterpretaciones que sólo causarán daño a la industria. Por último, aceptar una limitación como la relativa a la integridad en la cadena de suministro y a los riesgos asociados a ciertos proveedores y equipos, abre la puerta para que, en el futuro, se incluyan otras restricciones que no tengan base técnica y que se incluyan por motivaciones netamente políticas.
Artículo 13.	Continuación artículo 5… Chile debe seguir diversificando su matriz digital Nuestro país ha implementado un modelo que ha sido exitoso en el despliegue de redes y en el acceso de la población a las telecomunicaciones y, especialmente, a

	internet. El Estado ha impuesto las condiciones necesarias para que fueran los privados quienes invirtieran, a su riesgo, en el despliegue de redes y en la prestación de servicios. De esa manera, desde hace 3 décadas que Chile ha ido alcanzando niveles mayores de desarrollo en esta industria, liderando los rankings a nivel regional, pero aún con carencias propias de un país en vías de desarrollo, como aquellas relacionadas con la capilaridad y el despliegue de redes de alta velocidad en las zonas más alejadas de los grandes centros urbanos. Lo que ahora se requiere es pasar de una matriz de telecomunicaciones a una matriz digital, a esa supercarretera que hará posible ser parte de la 4ta revolución industrial. En virtud de ello, resulta incomprensible limitar la implementación de redes de algunos proveedores globales, ya que esa visión no forma parte de las políticas públicas económicas que ha seguido Chile en las últimas décadas. Muy por el contrario, al diversificar la matriz digital, Chile debe mantener las puertas abiertas a cualquier empresa, sea fabricante, operador de telecomunicaciones u operador de infraestructura. Sin embargo, si entrara en vigencia el borrador que nos ocupa, los operadores tendrán menores y peores opciones para implementar la tecnología 5G y las que vengan a futuro. En razón de lo anterior, resulta fundamental recibir siempre a las empresas e inversiones extranjeras para la entrada de las mejores y más modernas redes y tecnologías, lo que redundará en un mejor servicio a los consumidores.
Artículo 14.	Continuación artículo 5…

	Experiencia comparada Si miramos lo que están realizando los países desarrollados, nos encontramos con que la mayoría de ellos tienen políticas tecnológicamente neutrales en lo relativo a ciberseguridad de las redes de telecomunicaciones, las que se aplican a todos los fabricantes. Por ejemplo, Alemania (https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/ServicerProviderObligation/TelecommunicationSecurity/TelecommunicationSecurity_node.html) tiene una normativa estricta en ese sentido, a fin de no afectar el desarrollo de la industria ni de generar conflictos legales. En el caso alemán, elaboraron un catálogo con 10 criterios a seguir para los efectos de enfrentar estos riesgos desde un punto de vista neutral, dentro de los cuales se encuentran la obligación para cada proveedor de entregar información técnica y específica acerca de sus productos, o la obligación de cada proveedor de notificar inmediatamente a sus usuarios de cualquier vulnerabilidad que se presente en sus productos. Asimismo, es preciso señalar que las cadenas de suministro en el sector TIC no tienen un territorio de origen único. Un producto determinado (redes o dispositivos móviles) está formado por numerosos componentes de varios países. En consecuencia, desde la perspectiva de una división funcional global y de dependencia de una cadena de suministro, todos los proveedores tendrían el mismo riesgo en términos de ciberseguridad. Esto no hace más que reforzar la idea de la potencial discriminación que podría generarse con el borrador de norma técnica elaborado por Subtel.

	En virtud de la interdependencia global de la cadena de suministro, ¿es posible atribuir el concepto de riesgo a ciertos equipos y proveedores específicos que provengan de países individualmente considerados? Como es de común conocimiento, los fabricantes y proveedores más relevantes a nivel mundial se nutren de insumos y de investigación que se desarrolla en la mayoría de los continentes.
Comentarios Generales.	Atendida la importancia de la materia consultada, la cual requiere una evaluación detallada, agradeceremos prorrogar por el plazo de 15 días, el cierre del proceso de consulta (que vence el próximo 04 de junio de 2020), a fin de tener la posibilidad de formular consultas y opiniones sobre la propuesta de normativa de ciberseguridad, hasta el día 19 de Junio de 2020.
Comentarios Generales.	Eliminación de artículos específicos En virtud de lo señalado en los comentarios, se propone eliminar las siguientes frases y numerales: - artículo 5°, inciso segundo letra k), "determinaciones nacionales e internacionales en relación a los riesgos de seguridad asociados al uso de determinados equipos o proveedores", puesto que ello debe provenir de fundamentos técnicos que sigan directrices nacionales e internacionales ampliamente aceptados por la comunidad tecnológica, utilizando parámetros objetivos; - artículo 5°, inciso segundo letra l), "integridad de la cadena de suministros de equipos y software", ya que ello no contiene motivaciones estrictamente técnicas, además de que dicha cadena de suministro es de carácter global y no puede ser imputada a un proveedor

	en particular, como ya se ha demostrado en este mismo documento; - artículo 5°, inciso tercero, el vocablo “independiente”, ya que los planes de respuesta a que se refiere este inciso deben guiarse por estándares nacionales o internacionales, objetivos y de amplia aplicación, por lo que la inclusión de la palabra “independiente” no agrega valor al sentido de la norma, resultando confuso y objeto de malinterpretaciones; - artículo 5° inciso cuarto, la siguiente frase: “Asimismo, deberán adoptar todas las medidas que permitan verificar el cumplimiento eficaz de dichos criterios a lo largo de toda la cadena de suministros, pasando desde la manufactura de los equipos, su transporte y entrega, su instalación, su puesta en marcha y su entrada en servicio”; la eliminación propuesta se justifica dado que se ha solicitado precedentemente la eliminación de las letras k) y l) de artículo 5° inciso segundo, por lo que mantener esta redacción no tiene sentido para los fines de este artículo; - artículo 16°, inciso segundo, el vocablo “independiente”, toda vez que las pruebas de seguridad aludidas en dicho inciso, deben seguir los estándares actualizados, sean ellos nacionales o internacionales y que sean ampliamente aceptados por la comunidad tecnológica o las organizaciones multilaterales ligadas a la ingeniería y las telecomunicaciones. La inclusión de la palabra “independiente” solo lleva a confusión y genera problemas de interpretación no deseables para lo que se quiere regular.

	La propuesta de eliminar estas frases y vocablos tiene el único propósito de hacer consistente este borrador de norma técnica con los principios generales ya mencionados, con la historia normativa y con la jurisprudencia judicial y administrativa en la industria de las telecomunicaciones.