Juan Patricio Cristi Orellana (WOM)

Consulta 1: Atendidas las velocidades y coberturas expuestas en las tablas N°s 1 y 2, se le solicita opinar sobre este punto, en lo relativo a las bandas 700 MHz, AWS y 3.5 GHz.

"Contar con un portafolio diverso de bandas de frecuencias es relevante para la provisión de servicios, y es a lo que todo operador quisiera optar, pero ciertamente no es el único elemento que determina el nivel de eficiencia y calidad de servicio hacia los usuarios. Los hechos así lo demuestran: WOM ha sido un operador muy eficiente a pesar de tener menor cantidad de espectro y no contar con diversificación de bandas; esto lo ha logrado mediante inversiones sostenidas desde su ingreso a Chile; generando un quiebre positivo en la demanda de servicios móviles y resultando en el mayor receptor neto de clientes portados desde los Incumbentes: Entel, Movistar y Claro.

Es importante considerar que desde el punto de vista del usuario, la calidad de servicio percibida no se encuentra asociada necesariamente a una sola frecuencia, sino que es el resultado del conjunto completo de frecuencias de que dispone el operador. Es por esto que es esencial contar con un portafolio diversificado de espectro que permita complementar los beneficios diferentes que cada frecuencia provee. Lo anterior es consecuencia del principio de neutralidad tecnológica que tiene Chile y que permite el despliegue y reemplazo de tecnologías en una misma frecuencia, en la medida que ésta se encuentre desarrollada y el tamaño del bloque permita aprovechar las máximas prestaciones de cada nueva tecnología.

Por esto, considerar sólo la velocidad esperada parece ser insuficiente y ésta, además, no debiera depender de una banda de frecuencias específica sino que del total de espectro del que es titular un operador, considerando los distintos servicios específicos que se proveen.

En este contexto, la claridad del crecimiento y maduración de las frecuencias disponibles mediante un roadmap de espectro y la particular configuración y división de los bloques de espectro inciden directamente en las condiciones de competencia en su asignación.

Como lo señaló la FNE en su alegato ante el TDLC por la consulta de los CAP de espectro: “las características técnicas y la disponibilidad de equipos e infraestructura en cada frecuencia nos generan una restricción a como subdividir las bandas (…) por eso lo que se defina como tamaño de esos bloques puede llevar a que un determinado cap que este tribunal pueda fijar sea en definitiva o inviable técnicamente o irrelevante, en caso de que no se permita un diseño eficiente de bloques”.

Respecto de la Banda 700, para que un operador pueda lograr niveles mínimos de eficiencia tecnológica para la prestación de servicios de datos, necesariamente debe contar con un bloque completo de al menos 20 MHz. Así, en esta licitación, fraccionar el bloque resultaría ineficiente pues no permitiría a los operadores prestar servicios en condiciones competitivas. El Informe de Butelmann Consultores presentado en el proceso de consulta por los CAP de espectro compara el uso de la tecnología 4G en la banda 700 para bloques de distinto tamaño, concluyendo que “un operador con sólo 10 MHz de espectro en banda 700 no podría proveer servicios con tecnología 4G-LTE, (…) tendría desventajas para competir en términos de calidad de servicio, con operadores que cuenten con 20 MHz”.

En síntesis, es esperable que un operador que pueda utilizar un portafolio eficiente de bandas y con bloques de tamaño óptimo provea un servicio cuya velocidad sea superior a las registradas hoy en día. A modo de referencia, en el estudio de Tutela WOM lidera la experiencia móvil con 5517kbps."

Consulta 2: En consideración a la baja cobertura de bandas milimétricas, ¿qué criterio(s) considera adecuado(s) para evaluar los aspectos de velocidad y cobertura en la banda de 28 GHz?

"Para referirnos a este tema, es necesario precisar que una "optima transmisión o excelente servicio" (Art. 13C LGT) no es igual a alta velocidad y gran cobertura (aunque, en la práctica de las licitaciones, se hayan hecho sinónimos). En el caso de las bandas milimétricas, es dudoso que deban considerarse criterios de cobertura geográfica, debido a la ineficiencia en el despliegue en término de cantidad de antenas y superficie cubierta. Al respecto, podría ser más adecuado considerar una calidad de servicio mínima al utilizar estándar 5G (superior al que propone la Consulta Subtel ante el TDLC) y, por ejemplo, usar como variable de adjudicación la eficiencia espectral demostrada del postulante y un compromiso de nivel de inversión.

De igual manera, en la asignación de puntaje, no debiera castigarse de manera desproporcionada a aquellos operadores que no tienen red o tienen una red de cobertura menor que los operadores incumbentes. Una alternativa sería establecer como máximo puntaje por cobertura el despliegue de una red mínima para operar el servicio, como la alcanzada por operadores de menor tamaño o desafiantes.

Asimismo, creemos importante señalar que, de la mano con la regulación y posterior implementación del estándar 5G se debe realizar un análisis exhaustivo de los requisitos para despliegue de redes alámbricas (fibra óptica u otras) aguas arriba y de la Ley de Antenas (20.599). Lo anterior, debido a que las redes 5G requerirán de enlaces de alta disponibilidad y estabilidad, como lo es la fibra óptica, para aprovechar toda su potencialidad y además, se estima que las redes operando en estándar 5G requerirán de un número exponencialmente mayor a las antenas que existen hoy en día. Sin embargo, la Ley de Antenas ya genera problemas a los operadores: (i) Incorporó requisitos adicionales para para la instalación de torres; y (ii) aunque la Ley de Antenas contempla la colocalización, dicha obligación existe sólo para un número muy limitado de torres. Sólo hay obligación de celebrar contratos de colocalización respecto del parque de torres que se instale con posterioridad a la fecha de publicación de dicha Ley (11.06.12). Por ello, estimamos necesaria la coordinación del poder ejecutivo junto con el legislativo para crear una nueva normativa que permita desplegar mayor cantidad de antenas, ajustando los parámetros de protección, medioambiente y seguridad a los que ofrecerá esta nueva tecnología.

En esta misma línea, Subtel debiese proponer una actualización a los procedimientos relativos a concesiones y permisos de servicios de telecomunicaciones. El sistema actual tiene a las diversas divisiones de Subtel con una carga de trabajo excesiva, generando un perjuicio importante a la inversión nacional y extranjera, debido a la demora en los tiempos de respuesta de la misma autoridad. Teniendo en cuenta el aumento del número de antenas que

requerirán autorizar los operadores de telefonía móvil, la implementación de las redes 5G a través del sistema actual podría verse afectada de sobremanera.

Finalmente, estimamos que Subtel debe estructurar los bloques de espectro en las diversas bandas con el objeto de que sean técnicamente compatibles para prestar los diversos servicios, evitando así caer en un enfoque de sólo cobertura y velocidad, el que no ha dado los resultados esperados tal como sucede en el Proyecto FDT-2008-04, que obligó a una velocidad que hoy en día se encuentra obsoleta."

Consulta 3: Atendido que la cobertura de los proyectos técnicos se encuentra cautelada con la exigencia de un mínimo de velocidad de subida y de bajada, en cada banda, se le solicita opinar sobre este punto.

"Como se ha dicho anteriormente, sería recomendable profundizar y ponderar otros elementos además de la velocidad: total de espectro del que es titular el postulante, portafolio de frecuencias, tamaño de bloques, latencia, capacidad de red o throughput, entre otros. La capacidad es algo que el operador puede cumplir independientemente de la demanda de tráfico (que puede congestionar alguna celda y reducir la velocidad). También es más fácil de fiscalizar. En todo caso, la capacidad exigida debe depender de la cantidad de espectro que acumule el operador con el Concurso.

De igual manera, en la asignación de puntaje, no debiera castigarse a aquellos operadores que no tienen red o tienen una red de cobertura menor que los operadores incumbentes, por lo que nos parece que para que todos los concursantes puedan obtener el mismo puntaje por concepto de cobertura, el máximo puntaje por este ítem debe corresponder a lograr una cobertura equivalente a aquella alcanzada por operadores de menor tamaño o desafiantes.

Además, debería considerarse como elemento para asignación de puntaje un enfoque multivariado que incluya la eficiencia espectral alcanzada del último periodo que demuestre el postulante, normalizado por consumo promedio de datos de sus usuarios, cantidad de smartphones en su red, y todo ponderado según el tipo de macrobanda de las frecuencias que emplea para explotar los servicios.

Adicionalmente, el diseño de la licitación también incide directamente en las condiciones de competencia del mercado tras la asignación de espectro: “Las características del diseño de la subasta, como el formato de la oferta, el precio de reserva y la política de información (por ejemplo, la licitación anónima o transparente) también pueden influir en la competencia de la subasta. Por ejemplo, permitir ofertas por paquetes puede ayudar a los oferentes a agregar espectro de manera eficiente” (Cramton et. al. (2011). Using spectrum auctions to enhance competition in wireless services, Noviembre 2011, p. 172).

Si bien la licitación por paquetes de espectro o combinatorial permite licitar el mix de bandas particular que el oferente requiere, el diseño del concurso debe realizarse bajo reglas claras, no implicar una barrera adicional para operadores desafiantes o entrantes y evitar la adquisición de espectro con fines de acaparamiento o sin ánimo de uso efectivo.

Por ello, independiente del diseño del concurso, es esencial que la licitación propenda a que todos los operadores cuenten con un portafolio de espectro suficiente (en cantidad) y

diversificado (en distintas bandas de frecuencia) a efectos de obtener una igualdad de condiciones entre los operadores y con ello, suficiente presión competitiva en el mercado. Si en la Consulta Subtel se fijase un límite máximo de tenencia de espectro que, en definitiva, impida a operadores entrantes/desafiantes acceder a ciertas frecuencias y conformar un portafolio, sería relevante establecer, en cada licitación, la "reserva" de un determinado bloque para aquellos operadores que carecen de espectro en la banda específica que se licita (un operador de red sin portafolio y/o nuevo entrante). Si éstos no participaren en la licitación, cualquier operador móvil que cumpla con las condiciones específicas de la licitación podría luego adjudicarse el bloque de espectro."

Consulta 4: ¿Qué aspecto(s) considera relevante(s) para ser tratado(s) en materia de ciberseguridad?

"Se estima que una multiplicidad de servicios críticos serán soportados en redes 5G; dependencia que podría generar que un problema de ciberseguridad en esas redes tenga consecuencias graves.

En este contexto, los países, en la adopción de 5G, deben implementar medidas que garanticen la ciberseguridad de las redes vinculadas a ella de forma de proteger a sus ciudadanos, la continuidad de la industria, su soberanía y el desarrollo del país.

Teniendo en cuenta esto, los siguientes aspectos son relevantes para la implementación de 5G en Chile desde una perspectiva de ciberseguridad:

i. La implementación de 5G debe realizarse teniendo como eje la ciberseguridad

Chile debe establecer parámetros tendientes a garantizar la ciberseguridad de las redes 5G de los operadores mediante, al menos:

- Medidas técnicas y organizativas para la gestión de riesgos del ciberespacio.

- El reporte de incidentes de ciberseguridad, guardando coherencia con la regulación de la Ley 20.478 y el Decreto 60. Es necesario que se revise la conveniencia de asociar este reporte al sistema establecido en el Decreto 60, o implementar uno separado. Este sistema debe implementarse coordinadamente con los demás sistemas de reporte de incidentes implementados en el país o que se implementen en el futuro.

ii. La implementación de 5G a nivel normativo debe ser coherente con el marco regulatorio sobre ciberseguridad y la agenda legislativa

En Chile existen normas sobre ciberseguridad, incluyendo la propias de telecomunicaciones (Leyes 18.168 y 20.478, y Decreto 60), la PNCS, la Política Nacional de Ciberdefensa, y la Ley 19.628.

La agenda legislativa del gobierno contempla iniciativas sobre ciberseguridad que pueden impactar el funcionamiento de redes 5G, como el proyecto de ley sobre datos personales y el de delitos informáticos; así como los futuros proyectos: ley marco de ciberseguridad y ley de infraestructura crítica.

La autoridad, al establecer normativa, debe hacerlo guardando coherencia con las normas vigentes o aquellas que formen parte de la agenda legislativa.

iii. La implementación de 5G debe realizase bajo un marco normativo en ciberseguridad que promueva autorregulación

La Subtel debe reconocer que quienes mejor conocen la industria son los mismos operadores y, por ello, se deben promover las prácticas de autorregulación. Ya hay iniciativas en Chile que toman la autorregulación como herramienta útil que les permite ir adaptándose al cambio tecnológico.

iv. Las medidas regulatorias relativas a 5G deben ser eficientes en cuanto al reporte de incidentes y la coordinación con la autoridad

Las iniciativas regulatorias deben considerar modelos que reduzcan ineficiencias en la forma que los operadores se comuniquen con la autoridad para notificar incidentes de ciberseguridad.

Además, se debe buscar que los operadores no tengan que notificar o coordinarse con múltiples autoridades.

v. Las medidas regulatorias que se implementen relativas a 5G deben reforzar la seguridad de las cadenas de abastecimiento de los operadores

La implementación de 5G ha estado marcada por la seguridad de los componentes aportados por las cadenas de abastecimiento. Es relevante que la Subtel tome en consideración antecedentes imparciales que permitan un proceso de implementación competitivo y con eje en ciberseguridad.

vi. La implementación de 5G debe realizase aplicando políticas que eduquen y potencien las competencias de los usuarios y los trabajadores en ciberseguridad"

Consulta 5: ¿Qué condiciones específicas considera relevantes para la protección de IoT?

"Al conjugar el estado actual de la seguridad de los dispositivos IoT con la implementación de la tecnología 5G, estudios señalan que esto conllevaría un escenario de nuevos riesgos en ciberseguridad y en privacidad que se podrían sumar a los ya conocidos. Las siguientes consideraciones deberían ser tomadas en cuenta como mecanismos para contribuir a disminuir estos riesgos:

i. Evaluar la implementación de normativa que aborde las deficiencias de ciberseguridad en los dispositivos IoT que se comercialicen en el país y el de los que sean utilizados por los operadores que implementen redes 5G

Creemos recomendable analizar las siguientes normativas: (a) Resolución Subtel Exenta N° 3103-2012 que fija la norma técnica sobre requisitos de seguridad aplicables a antenas que generan ondas electromagnéticas; (b) Resolución Subtel Exenta N° 1463-2016 que fija la norma técnica que regula las especificaciones técnicas mínimas que deben cumplir los equipos

terminales utilizados en las redes móviles; y (c) Resolución Subtel Exenta N° 1985-2017 que fija la norma técnica de equipos de alcance reducido.

Para esto, se pueden tomar como ejemplo iniciativas comparadas:

- La Internet of Things Cybersecurity Improvement Act, que busca establecer que el gobierno federal de EE.UU. no adquiera equipos IoT que tengan problemas de ciberseguridad. En concreto, este proyecto establece un mínimo nivel de seguridad para cualquier dispositivo IoT que sea utilizado por el gobierno federal.

- La California's SB 327, que establece medidas de seguridad específicas para los fabricantes de dispositivos, como, por ejemplo, que cada contraseña preestablecida en un dispositivo sea única para ese dispositivo.

ii. Implementar políticas que permitan al mundo privado y público interiorizarse sobre IoT y cómo estos pueden conllevar riesgos de ciberseguridad distintos de los riesgos de los dispositivos TI convencionales

Se sugiere utilizar mecanismos de capacitación basados en guías técnicas basadas en estudios e investigaciones comparadas. Un ejemplo de una publicación realizada con el objetivo de difundir a las organizaciones sobre los dispositivos IoT y sus riesgos, es la que preparó el NIST de EE.UU. el año 2018. Esta publicación está dirigida al personal de las agencias federales con responsabilidades vinculadas a ciberseguridad.

iii. Aplicar políticas que permitan a los usuarios finales interiorizarse sobre el uso de los dispositivos IoT y cómo estos pueden conllevar riesgos de ciberseguridad

iv. Evaluar la adopción de estándares técnicos en materia de ciberseguridad en IoT

La ISO está elaborando la norma ISO/IEC WD 27030 que contendrá lineamientos para seguridad y privacidad relacionada específicamente con los dispositivos IoT.

Por su parte, el ETSI lanzó en febrero de 2019 su norma ETSI TS 103 645, que contempla un estándar de ciberseguridad para dispositivos IoT.

A nivel nacional, el INN todavía no ha emitido normas relativas a la seguridad en los dispositivos IoT, sin embargo, ya ha homologado de varias normas ISO vinculadas a la seguridad de la información.

v. Evaluar mecanismos para evitar alta congestión en el uso del espectro radioeléctrico

La tecnología 5G hará posible que millones de dispositivos estén operando activamente de manera continua, por lo cual va a ser necesario implementar medidas que puedan descongestionar el uso del espectro radioeléctrico, como, por ejemplo, implementando medidas para el apagado remoto de dispositivos IoT redundantes. "

Consulta 6: ¿Qué puntos considera importantes en materia de protección de datos personales, en relación con la tecnología 5G?

"La protección de los datos personales fue reconocida como una garantía constitucional el 2018. Por su parte, la Ley 19.628 establece dos bases de licitud para el tratamiento de datos personales: el consentimiento del titular y la ley. Al día de hoy, esta ley se ha visto superada por el avance tecnológico y, en ese contexto, se está discutiendo el proyecto de ley sobre datos personales que establece una regulación basada en el Reglamento Europeo de Protección de Datos.Desde la normativa de telecomunicaciones, existen resguardos a la confidencialidad e integridad de la información en el artículo 36B de la Ley 18.168.

La implementación de la tecnología 5G supondrá nuevos servicios y aplicaciones que pueden generar afectaciones a los derechos de los ciudadanos, incluyendo su vida privada y la protección de sus datos personales.

Las siguientes serían las principales afectaciones que a nivel de datos personales:

i. La tecnología 5G involucrará mayor disponibilidad y almacenamiento de datos de geolocalización de los usuarios.

Esta tecnología requerirá una mayor cantidad de antenas celulares. La proliferación de antenas hará susceptible la obtención de datos de geolocalización más precisos del usuario, resultando en una afectación a su privacidad.

Los datos de geolocalización en Chile son un dato personal en la medida que sean relativos a una persona natural (usuario), identificada o identificable. Por su parte, el proyecto de ley sobre datos personales establece un artículo sobre esta clase de datos, requiriendo informar al titular el tipo de datos de geolocalización que serán tratados, la finalidad y duración del tratamiento y si estos se comunicarán a terceros.

ii. La tecnología 5G puede involucrar riesgos a la privacidad de los datos de los usuarios derivados de ambientes compartidos.

En redes 5G, los recursos de la red son virtualizados y la infraestructura es compartida entre diferentes servicios de red y competidores. Estos ambientes compartidos pueden generar condiciones más favorables para el acceso no autorizado a datos personales de los usuarios.

iii. La tecnología 5G puede involucrar riesgos a la privacidad de los usuarios derivada de mayor dependencia en la tecnología cloud.

iv. La tecnología 5G puede involucrar riesgos a la privacidad de los usuarios asociados al hecho que esta tecnología masificará la utilización de IoT, los que son susceptibles de contener vulnerabilidades de software.

La combinación de 5G e IoT generará una producción mayor de datos personales de los usuarios de estos dispositivos, en áreas que hasta ahora habían sido ajenas a la digitalización.

Bajo este escenario, nos parecen relevantes las siguientes medidas:

i. Se debe modificar la normativa que regula el tratamiento de datos personales en Chile avanzando con la aprobación del proyecto de ley que modifica la Ley 19.628.

ii. Se deben evaluar mejoras regulatorias para los operadores, estableciendo parámetros técnicos y organizacionales de forma que se otorguen garantías en la protección de los derechos de los titulares de datos personales. Estos parámetros deben considerar varias aristas, como las características del operador, o la influencia que un tercer Estado pueda tener sobre él, su gobierno corporativo, etc.

iii. Se debe promover la autorregulación en la industria de telecomunicaciones. Los operadores pueden generar principios que reflejen consenso y que permitan las mejores prácticas en privacidad."

Consulta 7: ¿En qué sectores o actividades cree que los riesgos sobre la seguridad de la información pueden suponer un mayor freno para el proceso de transformación digital?

"Según diversos índices, la penetración de TIC en Chile es de las más altas en Latinoamérica. No obstante, estudios indican que todavía existirían brechas entre las empresas que han iniciado su proceso de transformación digital, respecto de las que no.

De acuerdo con el Índice de Transformación Digital de Empresas (2018) dos tercios de las empresas (esencialmente pymes) no han dado pasos hacia la transformación digital. Este estudio es coherente con la última Encuesta Longitudinal de Empresas del Ministerio de Economía que señala que solo el 24,5% de las empresas que utiliza internet realizaron comercio electrónico el 2017.

La situación de las pymes en Chile y su brecha en transformación digital no es distinta de lo que ha ocurrido en otras latitudes. El informe OCDE sobre transformación digital en el G20 establece dentro de sus recomendaciones que los países apoyen a las pequeñas y medianas empresas para que puedan abordar los desafíos que esta transformación presenta.

En este contexto, las pymes en Chile parecieran ser uno de los sectores donde los riesgos sobre ciberseguridad pueden suponer un mayor freno para la transformación digital; esto, en comparación de aquellos sectores donde la transformación digital está más avanzada (grandes empresas y sectores regulados) y, por lo tanto, donde la conciencia de los riesgos inherentes al mundo digital está ya afianzada.

Esta hipótesis se sostiene en las cifras señaladas, en consideración a que el proceso de transformación digital en parte importante de pymes en Chile es nulo o primitivo a la fecha. En este sentido, es razonable concluir que una entidad análoga difícilmente tendrá políticas o una cultura relacionada con ciberseguridad de activos digitales cuando no tiene en su operación tales activos.

Esta situación puede verse también favorecida por el hecho que en Chile no existen normativas sobre ciberseguridad que se relacionen con las pymes o autoridades supervisoras en el tema, como sí lo tiene, por ejemplo, el sector bancario.

Nuestra hipótesis no plantea que el proceso de transformación digital no pueda verse retrasado en otras industrias por tener un proceso ya avanzado. Hemos sido testigos de ciberataques que han involucrado entidades cuyo proceso de transformación digital se había desarrollado dejando de lado la ciberseguridad y que, sin duda, impactaron en la velocidad de

avance de su proceso de transformación digital. El núcleo de nuestra respuesta es que el grado de retraso en el proceso de transformación digital que puede involucrar a una pyme va a ser mayor que el que pueda sufrir una gran empresa ante un ciberataque, aun cuando en este último caso también se produzcan impactos.

Algunas medidas para abordar esta situación serían las siguientes:

i. Incorporar políticas de capacitación y educación en ciberseguridad, y en los beneficios de la adopción de tecnologías digitales: digitalización y ciberseguridad deben ir de la mano.

ii. A nivel indirecto, creemos que se debe avanzar en la transformación digital de la Administración del Estado. La transformación digital a este nivel puede tener importantes efectos en la forma que las empresas y ciudadanos se relacionan con el Estado, siendo más eficiente, más transparentes, y con menos burocracias, todo lo cual genera menos cargas para las pymes."

Consulta 8: ¿De qué manera debería implementarse la ciberseguridad a nivel de interfaz de radio e infraestructura de red?

"El sistema 5G es una evolución de los sistemas de comunicaciones móviles 4G. En consecuencia, la arquitectura de seguridad 5G está diseñada para integrar seguridad 4G equivalente. Además, la reevaluación de otras amenazas de seguridad, como los ataques a las interfaces de radio, el plano de señalización, el plano del usuario, el enmascaramiento, la privacidad, los problemas de seguridad entre operadores e interoperadores también han sido tomados en cuenta para 5G y dará lugar a nuevas mejoras de seguridad. El grupo de trabajo 3GPP participa activamente en la determinación de los requisitos de seguridad y privacidad, y en la especificación de las arquitecturas y protocolos de seguridad para 5G. La Open Networking Foundation (ONF) está dedicada a acelerar la adopción de SDN (software defined networks) y NFV (network functions virtualization) y a publicar especificaciones técnicas para la seguridad, incluidas las especi¿caciones de seguridad de las tecnologías.

5G puede y será una piedra angular en la realización de la visión de la sociedad de la información, en el que todo lo que puede beneficiarse de una conexión se conectará. Pero en lugar de abordar la seguridad 5G al intentar implementar todos los mecanismos de seguridad imaginables, es necesario que haya un enfoque sistemático y analítico de múltiples partes interesadas, anclado en un nuevo modelo industrial de seguridad para redes 5G."