Respuesta de Derechos Digitales a consulta ciudadana:
Lineamientos del concurso público que otorga permisos de servicio limitado de telecomunicaciones para el despliegue y provisión de soluciones de comunicación mediante el uso de tecnología 5G

Preguntas 1 a 5 no fueron contestadas por no pertenecer al ámbito de trabajo de la organización.

Respuesta a pregunta 6. Con el fin de evaluar las mejores condiciones técnicas que aseguren una óptima transmisión o excelente servicio, ¿cuáles cree Ud. que debieran ser los elementos a considerar por la Subsecretaría de Telecomunicaciones para discriminar entre diferentes postulaciones para una misma zona de servicio en las bandas de frecuencia medias y altas?

A. Contexto

La telefonía móvil de quinta generación (5G) ha sido presentada como la promesa de desarrollo futuro de las telecomunicaciones, ello atendida su mayor velocidad (para mover más datos), menor latencia (para ser más receptivo) y la capacidad de conectar muchos más dispositivos a la vez (para sensores y dispositivos inteligentes) que prometen abrir las puertas al desarrollo de la inteligencia artificial, los vehículos autónomos, la realidad virtual o aumentada, y al Internet de las Cosas (IoT), creando hogares, industrias y ciudades inteligentes.

La expectativa es que 5G permita un amplio despliegue de funciones de comunicación en todas las áreas en que los individuos se desarrollan y relacionan, incluido el Estado, la industria, el comercio, la seguridad nacional interna y externa, la provisión de servicios básicos, entre otros.

Se prevé incluso que una multiplicidad de servicios críticos serán soportados en redes que implementen tecnología 5G, lo que hace aun más necesario reforzar las consideraciones de seguridad de las mismas, ya que cualquier vulnerabilidad de las mismas tendrá consecuencias graves en la vida cotidiana de la población e incluso en la soberanía del Estado. Como lo apunta la Política Nacional de Ciberseguridad (PNCS), *"es necesario promover el resguardo de las redes y sistemas informáticos del sector público y privado, especialmente aquellas que son esenciales para el adecuado funcionamiento del país, velando por la continuidad operacional de los servicios básicos".*[1]

Se requiere prioritariamente establecer los estándares y protocolos comunes sobre cómo van a operar nuestras telecomunicaciones en las próximas décadas. Los diferentes aspectos de la tecnología a implementar merecen ser abordados con detención para prevenir afectaciones a los derechos de los ciudadanos, incluyendo las garantías constitucionales relativas a la vida privada, la protección de sus datos personales, la inviolabilidad de las comunicaciones, la libertad de expresión y el acceso a la información.

[1] Política Nacional de Ciberseguridad, disponible en <https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf> p. 12.

No basta con las consideraciones de eficiencia u óptima transmisión para evaluar la excelencia del servicio, dadas por la capacidad de la tecnología de capturar y procesar mucha información a través de una multiplicidad de dispositivos y técnicas de big data, si no que la calidad de excelencia de servicio debe apuntar prioritariamente a la adecuada protección de los derechos, y acorde con ello exigir la adopción de medidas de ciberseguridad alineadas con la protección integral de tales derechos de las personas que interactúen en cualquier forma con los servicios posibilitados por la tecnología 5G. En tal sentido, y tal como se establece en la PNCS: *"Es necesario brindar a las personas un nivel de seguridad que les permita el normal desarrollo de sus actividades personales, sociales y comunitarias en el ciberespacio, junto con el ejercicio de derechos fundamentales como la libertad de expresión, el acceso a la información, la protección de la vida privada y la propiedad"*.[2]

La misma PNCS establece como uno de sus objetivos que deben ser satisfechos por diferentes políticas públicas: *"el desarrollo de procesos de análisis y gestión de riesgos que permitan identificar las vulnerabilidades, amenazas y riesgos implícitos en el uso, procesamiento, almacenamiento y transmisión de la información, junto a la generación de las capacidades para la prevención y la recuperación ante incidentes de ciberseguridad que se presenten, configurando un ciberespacio estable y resiliente"*.[3] Tal exigencia resulta plenamente aplicable a las condiciones de excelencia de los servicios 5G cuyos permisos se busca licitar.

B. <u>Principales riesgos para el ejercicio de derechos que presenta la implementación de la red 5G que deben ser abordados por SUBTEL a través de exigencias de servicio de excelencia a los postulantes a dichas frecuencias</u>

1. Mayor almacenamiento y eventual disponibilidad de datos de geolocalización de usuarios. Conforme a la Ley Nº19.628 los datos de geolocalización de un usuario son en Chile un dato personal en la medida que estos son relativos a una persona natural (usuario), identificada o identificable.

La tecnología 5G requiere para su implementación una gran cantidad de antenas celulares posicionadas a corta distancia en consideración a que sus señales tienen un rango de señal menor que el de otras tecnologías. La mayor concentración de antenas hará posible verificar de forma más precisa la geolocalización de los usuarios de telefonía móvil, y esta información sensible puede ser fácilmente utilizada por gobiernos, empresas y agentes maliciosos, resultando en una afectación a la privacidad de sus titulares.

Si lo anterior se combina con disposiciones regulatorias que extienden el plazo de retención de tales datos –como hoy se debate en el Congreso como parte de la actualización de la normativa de delitos informáticos- los datos de geolocalización de los usuarios de esta red se encontrarán disponibles por un periodo mayor con una granularidad que pondrá en riesgo adicional a sus titulares, y que por tanto debe ir acompañado de medidas reforzadas de parte de la operación del proveedor de servicios para cautelar su seguridad, y acceso limitado y acorde a las exigencias legales vigentes.

[2] Ibid.
[3] Ibid.

2. Riesgos de seguridad mediante la degradación de operación a 5G para su comunicación con redes 4G, 3G o incluso 2G, y otras técnicas en constante descubrimiento por expertos técnicos. Los protocolos 5G han actualizado los estándares para proteger la comunicación entre los dispositivos y las antenas, aportando algunas mejoras que deberían evitar el abuso de los protocolos de señalización (necesarios para el *roaming*) o el despliegue de receptores IMSI para recopilar metadatos, lo que implica mejoras de seguridad respecto de otras redes. Sin embargo, ya que los nuevos protocolos 5G tendrán que coexistir con otros más antiguos, tales como 4G, 3G o incluso 2G, y esos protocolos aún son vulnerables, ello resulta en riesgos de seguridad aún para aparatos que funcionan en 5G. Esto sucede debido a un ataque de degradación, donde se engaña a los dispositivos para que funcionen en protocolos más antiguos, o debido a la falta de disponibilidad de redes 5G, o finalmente, porque algunos dispositivos están diseñados para operar en redes más antiguas, como dispositivos de pago o sistemas de control industrial. Nuevas vulnerabilidades continúan siendo encontradas y reportadas por investigadores constantemente.[4]

3. Riesgos a la privacidad de los datos de los usuarios derivados de ambientes compartidos a través del almacenamiento de información en la nube. En redes 5G, los recursos de la red son virtualizados y la misma infraestructura es compartida entre diferentes servicios de red y competidores. Como lo explica Benusi, "según señalan algunos autores, estos ambientes compartidos pueden generar condiciones más favorables para el acceso no autorizado a datos personales de los usuarios".[5] La utilización de ambientes compartidos y la multiplicación de dispositivos conectados a la red genera condiciones más favorables para el acceso no autorizado de datos personales.

4. Tecnología 5G facilitará la implementación masiva de dispositivos IoT, que de no adoptarse protocolos de privacidad y seguridad estrictos son altamente susceptibles a vulnerabilidades de software y hardware. Los dispositivos IoT recolectan datos personales de sus usuarios en áreas que hasta ahora habían sido ajenas a la digitalización. Por ello, la red 5G que permite la transmisión, almacenamiento y procesamiento de esta información puede generar riesgos a la privacidad del usuario que hasta ahora no existían. La ciberseguridad de los dispositivos IoT es materia de creciente preocupación en los últimos años, se ha desarrollado investigación y estándares técnicos que apuntan a abordar en forma preventiva las vulnerabilidad de dispositivos IoT en el mercado, entre las cuales puede enumerarse: otorgar acceso no autorizado a información de carácter sensible o datos personales, la utilización de los dispositivos como zombis para ataques masivos de denegación de servicio, la utilización de los dispositivos para vigilancia dirigida o masiva de grupos de la población, entre otros.

La expansión de 5G con sus sensores inteligentes conectados a ella permite prever un aumento exponencial de riegos en las fallas de diseño de software y hardware, desde credenciales codificadas, donde algunos dispositivos tienen una 'contraseña maestra' que cualquiera puede explotar, hasta vulnerabilidades sin parches que permiten a atacantes expertos controlar

[4] Ver Altaf Shaik y Ravishankar Borgaonkar. "New Vulnerabilities in 5G Networks", disponible en <https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf>

[5] Carlo Benussi, "La tecnología 5G y su impacto en la privacidad", Hipervínculos, 6 de junio de 2019, disponible en: <https://www.hipervinculos.cl/la-tecnologia-5g-y-su-impacto-en-la-privacidad/>

dispositivos sin importar cómo estén configurados, como sucedió con el tristemente celebre ransomware Wannacry.

Dispositivos siempre conectados pueden traducirse en usuarios impotentes, lo que los expone a un riesgo permanente de abuso. La tecnología 5G permite una relación directa entre el fabricante del dispositivo con los proveedores móviles que permiten su conectividad, dejando a los usuarios sin control alguno sobre sus dispositivos conectados. En el ejemplo compartido por Francisco Vera, un proveedor de un electrodoméstico inteligente que compramos con cuotas de crédito podría decidir no funcionar a menos que estemos al día con sus cuotas.[6] Lo mismo podría ocurrir a una línea de producción de una industria inteligente morosa de pago de su equipamiento. ¿Y si el servicio se refiere al procesamiento de muestras médicas urgentes para un diagnóstico de salud?

5G sin una adecuada regulación puede facilitar una subversión a través de mecanismos técnicos del ejercicio de muchos derechos que van desde alterar el significado de la propiedad, transformando a los dispositivos en un servicio sobre el cual no se tiene control, a la alteración constante de la privacidad, la inviolabilidad de las comunicaciones y la libertad de expresión, a través de un monitoreo constante e invisible a su existencia para el usuario.

5. Concentración de servicios en áreas ya servidas y profundización de brecha de servicios para zonas excluidas. Al utilizar frecuencias milimétricas, el 5G es increíblemente caro de implementar. Incluso en condiciones ideales, requiere que las antenas se instalen a muy poca distancia la una de la otra. Esto no sólo hace que sea muy difícil instalar esta infraestructura en zonas rurales, sino que también implica que probablemente más recursos económicos y humanos estarán enfocados en implementar 5G, en desmedro de extender la cobertura a zonas que todavía no cuentan con conectividad. En otras palabras, mejor conexión para los ya conectados. Si bien este riesgo no puede ser mitigado por las condiciones de concesión de permisos 5G, resulta un elemento que SUBTEL debiera tener a la vista a la hora de asegurar una eficiente asignación del espectro, que de cabida al desarrollo de diferentes modelos de negocios que puedan estar más acorde al desarrollo de zonas tradicionalmente excluidas o sub-servidas. Derechos Digitales ha provisto recomendaciones de política pública en tal sentido.[7]

C. Recomendaciones respecto a elementos a considerar en la excelencia del servicio en todas las frecuencias 5G

Cualquier asignación de permisos 5G por SUBTEL debe considerar como elementos esenciales de la excelencia del servicio la ciberseguridad y la protección de datos personales, que propicien la adopción estándares internacionales de seguridad en la operación de IoT.[8]

[6] Francisco Vera, "Welcome to 5G: Privacy and security in a hyperconnected world (or not?)", disponible en <https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not>

[7] Marianne Díaz, "Marcos regulatorios para las redes comunitarias: Argentina, Brasil, Colombia y México", 2018, disponible en <https://www.derechosdigitales.org/wp-content/uploads/redes-comunitarias-2018.pdf>

[8] Tales como ETSI TS 103 645 que ha sido propuesto por el Comité Técnico de Ciberseguridad (TC CYBER) del Instituto Europeo de Normas de Telecomunicaciones (ETSI), un estándar para la ciberseguridad del internet de las cosas, que permite establecer una línea de base de seguridad para productos de consumo conectados a Internet y proporcionar una base para futuros esquemas de certificación IoT, disponible en: <https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf>

En concreto, nuestras recomendaciones al respecto son las siguientes:

- Los elementos de evaluación deben incentivar el uso de protocolos de comunicaciones seguros, incluido el uso de estándares de cifrado sólidos.
- Los elementos de evaluación deben considerar las medidas concretas operativas por las cuales los servicios licitados acrediten el cumplimiento de la normativa de protección de datos personales vigente en el almacenamiento, procesamiento y comunicación de datos de geolocalización y otros datos personales recolectados por los dispositivos conectados a ellos.
- Los elementos de evaluación deben incentivar la aplicación de medidas técnicas concretas relativas a la protección de la privacidad de los usuarios, como, por ejemplo, privacidad por diseño, evaluaciones de impacto asociadas a privacidad de los servicios desplegados previo a su implementación, y auditorías periódicas de seguridad realizadas por terceros auditores durante su prestación, entre otros.[9]
- Se debe evaluar el ejercicio de la potestad reglamentaria de SUBTEL para el desarrollo de normas específicas para las empresas de telecomunicaciones que provean este tipo de servicios 5G, estableciendo parámetros mínimos a nivel técnico y organizacional que deban cumplir los operadores de forma que otorguen garantías en la protección de los datos personales de los usuarios, incluyendo medidas estrictas en confidencialidad de la información, e informes de transparencia obligatorios de las empresas proveedoras a sus usuarios en relación al origen de los componentes (hardware) y software que determinan el nivel de seguridad de la tecnología 5G ofrecida.[10]

La tecnología 5G puede resultar realmente revolucionaria, sin embargo, ello mismo exige una actualización del marco normativo y un ejercicio activo de las potestades de SUBTEL para asegurar que dicha implementación se realice en forma tal que se potencien sus beneficios y se limite los riesgos de afectación de derechos que han sido aquí examinados.

Atentamente,

María Paz Canales Loebel
Directora Ejecutiva
ONG Derechos Digitales

Santiago, 7 de noviembre 2019

[9] Ver las recomendaciones de la conferencia internacional sobre seguridad de las redes 5G o "Propuestas de Praga", de 3 de mayo de 2019, disponible en: <https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf>
[10] Este tipo de intervención regulatoria ha sido sugerida en los Estados Unidos por el Senator Ron Wyden quien con fecha 6 de noviembre de 2019, envió una carta a la Comisión Federal de Comunicaciones (FCC), que puede leerse aquí: <https://www.wyden.senate.gov/imo/media/doc/110619%20Wyden%205G%20Security%20Letter%20to%20FCC.pdf>