El despliegue de las redes 5G, o la geopolítica digital

Vicente Moret Millás | Letrado de las Cortes Generales, Letrado de la Comisión Mixta de Seguridad Nacional y profesor asociado IE Law School.

Tema

El despliegue de las nuevas redes de comunicaciones 5G está poniendo de relieve la existencia de una competición geopolítica por el control e implantación de las nuevas tecnologías.

Resumen

La tecnología 5G es la que permitirá el pleno desarrollo del Internet de las cosas (IoT), la conducción autónoma, la impresión 3D, la industria 4.0, la telemedicina, el uso masivo del *Big Data*, la robótica avanzada o la realidad virtual, entre otras realidades de la economía digital. En 2020 todos los países de la Unión Europea (UE) deberán disponer de, al menos, una ciudad principal con tecnología 5G disponible comercialmente y, la cobertura deberá ser total en 2035. El despliegue, según la Comisión Europea, aportará 910.000 millones de euros adicionales al PIB de la Unión y la creación de 1,3 millones de puestos de trabajo. Sin este esfuerzo inversor no se logrará un mercado único digital y Europa quedaría por detrás de Estados Unidos y China en la carrera por el dominio tecnológico mundial. La competición de fondo se traduce en prácticas proteccionistas, en sospechas sobre el cumplimiento de las normativas sobre privacidad o propiedad industrial de algunos fabricantes, o en denuncias de que esa tecnología disponga de puertas traseras que permitan acciones no deseadas sobre sistemas integrados en infraestructuras relevantes para la seguridad nacional.

Análisis

La próxima disrupción digital

Conseguir conexiones a internet rápidas y fiables constituye ya un objetivo prioritario para cualquier país que quiera no perder el tren de la nueva economía digital. Esta conectividad es ya un factor de competitividad clave para la economía de los estados, al igual que lo han sido en el pasado otras infraestructuras no digitales como las de energía o las de transporte. La propia UE lo ha entendido así al lanzar, en septiembre de 2016, una iniciativa derivada de los objetivos marcados por el presidente de la Comisión Jean-Claude Juncker en el debate del Estado de la Unión.[1] A raíz de este impulso, la UE entiende que no puede quedarse atrás respecto a otros actores como Estados Unidos y China en la configuración de un futuro digital para Europa.

[1] Jean-Claude Juncker, Discurso sobre el Estado de la Unión (2016), "Hacia una Europa mejor: una Europa que proteja, empodere y vele por la seguridad", 14/IX/2016, http://europa.eu/rapid/press-release_SPEECH-16-3043_es.htm.

Central en este impulso es lograr un despliegue adecuado, rápido y fiable de las redes de comunicación 5G. Así, los objetivos señalados a este respecto consisten en lograr acceso a una conectividad de velocidad extremadamente alta (1Gigabit de datos por segundo) en los centros socioeconómicos importantes tales como centros educativos, nudos de transporte, proveedores de servicios públicos y otros. Además, todos los hogares europeos deberán contar al menos con una velocidad de descarga de 100 Mbps. No obstante, todo ello sólo será posible si todas las zonas urbanas, las carreteras y los ferrocarriles disponen de cobertura ininterrumpida de 5G, lo cual supone transitar hacia la quinta generación de sistemas de comunicaciones inalámbricas. Según la UE, en 2020 todos los países de la deberán disponer de, al menos, una ciudad principal del Estado con 5G disponible comercialmente y en 2025 el despliegue deberá ser total. Las inversiones que requiere esta nueva red suponen para Europa, según la Comisión Europea, 910.000 millones de euros adicionales al PIB de la Unión y la creación de 1,3 millones de puestos de trabajo. Sin este esfuerzo inversor no se logrará un mercado único digital y Europa quedaría por detrás de EEUU y China en la carrera por el dominio tecnológico mundial.

Ahora bien, si es tan importante no perder esa importante carrera, cabe plantearse qué hace tan relevante desde el punto de geopolítico una cuestión aparentemente, y en puridad, sólo tecnológica. La conectividad 5G no es simplemente una mejora a lo ya existente como en su día supuso el paso del 3G al 4G, es un auténtico cambio profundo en la conectividad que va a permitir, entre otras cosas, un tiempo de respuesta de la red de un milisegundo y una velocidad de conexión 100 veces más rápida que la actual red 4G, además de permitir ahorrar energía en un 90% respecto a los sistemas actuales.

En definitiva, esa velocidad y fiabilidad de la conexión va a ser, como afirma el Plan Nacional 5G aprobado por el Gobierno de España en 2018,[2] una pieza clave en la transformación digital de la sociedad y la economía de los países avanzados, ya que el pleno desarrollo del Internet de las cosas (IoT), la conducción autónoma, la impresión 3D, la industria 4.0, la telemedicina, el uso masivo del *Big Data*, la robótica avanzada o la realidad virtual, entre otras realidades, se soportará sobre la base del 5G. En definitiva, todas las grandes innovaciones previstas para los próximos años, que son la base de la denominada economía del dato, sólo serán posibles si previamente se ha desplegado con éxito toda la infraestructura y sistemas necesarios para disponer de esa tecnología 5G.

Se espera que este despliegue alcance su madurez tecnológica y comercial a partir de 2020 y que su impacto mejore la productividad, la eficiencia y la eficacia de empresas y administraciones públicas logrando un efecto de impulso económico transversal sobre el conjunto de la economía. Los sectores que se señalan como más favorecidos serán los de industria, automoción, seguridad, defensa, salud, medios de comunicación y entretenimiento, energía, transportes y servicios financieros. Los requisitos para ese despliegue son técnicos y económicos. El modelo elegido en la mayoría de los países para el despliegue de esta red y asegurar la viabilidad económica, consiste en permitir a los operadores que celebren acuerdos voluntarios entre ellos para la distribución,

[2] Plan Nacional 5G. 2018-2020, Secretaria Estado para la Sociedad de la Información y Agenda Digital, METAD, 2017, https://avancedigital.gob.es/5G/Documents/plan_nacional_5g.pdf.

colocación y uso compartido de las costosas infraestructuras, casi siempre sobre la base de un operador dominante que permite utilizar sus recursos a los demás operadores sobre la base de acuerdos y compensaciones. Es necesaria una gran inversión que deberá ser costeada por las empresas privadas de telecomunicaciones que asuman ese reto. Y ello porque es necesario desplegar infraestructura adicional a la ya desplegada con el 4G: más fibra e instalar miles de *"small cells"* cada centenar de metros para cubrir todo el territorio. Además, las administraciones públicas deberán asegurar una correcta gestión del espectro radioeléctrico, que es de dominio público, con el objeto de liberar ancho de banda.

Geopolítica y redes de comunicaciones

No obstante, lo más relevante de toda esta cuestión, aparentemente sólo tecnológica, es que, como ponen de manifiesto recientes acontecimientos en la esfera internacional, lo que está en juego es algo más que una correcta utilización de las enormes oportunidades que ofrece la tecnología para mejorar las cosas. Lo que también está en juego es la preponderancia tecnológica que, una vez más, se convierte en campo de enfrentamiento geopolítico entre las grandes potencias. Así lo han entendido en los últimos años Estados Unidos y China, países ambos metidos de lleno en una carrera para lograr la supremacía tecnológica en abierta competencia geopolítica. Y este enfrentamiento que es económico, tecnológico y comercial, también afecta a la seguridad nacional. La prevalencia de las tecnologías y sistemas otorga a aquel que logra esa posición una ventaja competitiva indudable a la hora de poder imponer sus intereses geopolíticos, económicos, comerciales o incluso culturales. Por ello la seguridad nacional de los Estados también está implicada en el caso del resto de los países y no solo para esas superpotencias, ya que la dependencia tecnológica o la opción por unos u otros sistemas pueden ser opciones estratégicas que condicionen el futuro desarrollo de esos países.

De hecho, el 5G también se ha convertido en arena conflictiva en la cual las dos potencias compiten en una auténtica guerra comercial, utilizando en ocasiones razones de seguridad nacional que, probablemente, también incluyen una buena dosis de protección a empresas nacionales y disputa por la imposición de la tecnología propia. No es de extrañar que esa disputa se haya agudizado en el último año porque es mucho lo que está en juego. Forma parte del conflicto abierto más amplio e importante relativo a los microchips. Estos se encuentran ahora dentro de todos los dispositivos que nos rodean. Si los datos son el nuevo petróleo, los chips son los motores que hacen que ese combustible sirva para algo. El primero de los ámbitos en los cuales esa clave tecnológica se manifiesta es en todo lo relativo a la industria de seguridad y defensa, consumidora masiva de microchips que son críticos para todos los sistemas. Esta preocupación se ha puesto de manifiesto recientemente en la Estrategia de Seguridad Nacional de EEUU aprobada en diciembre de 2017.

En el ámbito del despliegue de las redes 5G va a tener una especial relevancia la fabricación de las *small cells,* que van a ser parte importante de la arquitectura del sistema. A este respeto hay que destacar que son cinco los fabricantes principales de estos elementos: Nokia, Ericsson, Samsung, Huawei y ZTE, las dos últimas empresas chinas. Es, precisamente, esa la razón por la que la utilización de tecnología de estas

dos empresas ha producido notorios y graves enfrentamientos en el ámbito de las relaciones comerciales y políticas entre EEUU y China. Así, este mismo año el gobierno de Estados Unidos prohibió por un tiempo a las empresas norteamericanas que suministrasen componentes a la empresa china ZTE para sus equipos de telecomunicaciones debido a la ruptura de un acuerdo previo de no vender esa tecnología a Irán.

No obstante, esa disputa geopolítica se refiere sobre todo a la posibilidad de que fabricantes chinos introduzcan en sus productos dispositivos que permitan el envío de información de forma encubierta o que, sencillamente, puedan escapar al control del operador de esos equipos poniendo en peligro la seguridad, integridad o confidencialidad de los sistemas. Ya en 2012, la Comisión de Inteligencia del Congreso de los Estados Unidos avisó que tanto ZTE como Huawei podrían ser una amenaza para la seguridad nacional.[3] Otra manifestación de esa preocupación sería, por ejemplo, la prohibición por parte del gobierno de Nueva Zelanda dirigida a un operador de redes de telecomunicaciones, Spark, sobre la utilización de sistemas de la empresa Huawei para el despliegue de su red 5G. Se convierte así un asunto tecnológico en una cuestión de seguridad nacional y, al mismo tiempo, se siguen los pasos de Australia y Estados Unidos que ya impiden que el equipamiento de ese fabricante se integre en sus redes de comunicaciones. Recientemente Alemania se ha unido a este veto a la tecnología china para el despliegue de las redes 5G alegando razones de ciberseguridad. Por ello, China afirma que Estados Unidos están presionando a sus aliados para que tomen partido en esta nueva guerra tecnológica.

La Administración estadounidense se ha mostrado preocupada por la ciberseguridad de las nuevas redes frente a posibles intromisiones o disrupciones producidas por gobiernos extranjeros sobre la base previa de un caballo de Troya tecnológico. Para prevenir el riesgo, el Consejo Nacional de Seguridad elaboró un informe para crear una nueva red 5G nacional construida, gestionada y controlada por el Gobierno de los EEUU, no por ninguna empresa privada. Aspiraba a crear una red 5G segura que se contrapusiese a la posición dominante de China en la fabricación y uso de infraestructuras de red. Se proponían nuevos estándares de seguridad para lograr un nuevo paradigma de ciberseguridad que, además, trataban de atraer a esa nueva red a los países aliados de EEUU. Las filtraciones previas a la prensa de la intención de la Administración Trump generaron una controversia.[4] No obstante todo lo anterior, la iniciativa de nacionalización de la red 5G fue rechazada de plano por ser costosa y cambiar totalmente el esquema de despliegue que ya se está llevando a cabo en EEUU por parte de operadores privados. Finalmente, el presidente Trump elaboró un memorándum presidencial para regular el desarrollo del espectro.

[3] "U.S. Panel Cites Risks in Chines Equipment", *The New York Times*, 8/X/2012, https://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

[4] "Trump team idea to nationalize 5G network to counter China is rejected", *Reuters*, 29/I/2018, https://www.reuters.com/article/us-usa-trump-5g-fcc/trump-team-idea-to-nationalize-5g-network-to-counter-china-is-rejected-idUSKBN1FI1T2.

En definitiva, el despliegue de las redes 5G es una materia de suma importancia tecnológica, pero también económica para lograr un tránsito hacia la economía digital y social por las grandes consecuencias del disruptivo proceso de transformación de las comunicaciones. Junto a las anteriores, el despliegue de la quinta generación de comunicaciones 5G forma parte del enfrentamiento entre países por lograr una posición de preponderancia en esa nueva etapa de desarrollo tecnológico. En ese sentido, son evidentes los enfrentamientos y alineamientos que se están produciendo como consecuencia de esa disputa que colocan las cuestiones relativas a la ciberseguridad de los sistemas como punto crucial, pero que muy probablemente también incluye asuntos de política comercial en relación con un mercado, el de los microchips, valorado en 412.000 millones de dólares en 2017, un 21% más que en 2016. Un mercado que no hará más que crecer en los próximos años debido a la incorporación masiva de microchips en dispositivos conectados a la red. Según estimaciones de la UTI, organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación, en 2019 en el mundo habrá 25.000 millones de dispositivos conectados a la red[5]. Se calcula que esa cifra ascenderá a 75.500 millones en 2025. Las cifras hablan a las claras de la relevancia de alcanzar una posición de superioridad en ese mercado.

Conclusiones

En definitiva, parece que una nueva guerra fría tecnológica está configurando bloques mundiales alrededor de los sistemas de telecomunicaciones que se utilizan, en un capítulo más de la disputa por la creación y uso de la tecnología, como fuente de crecimiento económico y seguridad militar.

Los aspectos relativos a la ciberseguridad de redes y sistemas son esenciales para asegurar el desarrollo de la economía mundial. Así, en su informe sobre riesgos globales el Foro Económico Mundial de Davos de 2019 señaló los ciberataques como la amenaza más probable solo por detrás de los eventos climatológicos extremos, de los desastres naturales y el robo masivo de datos. No obstante, lo que no parece serio es restringir las libertades económicas que amparan el libre comercio mundial sin motivos sólidos, fundados y no apriorísticamente determinados por categorías completas de empresas según la nacionalidad. Existen serias sospechas sobre el cumplimiento de las normativas sobre privacidad o propiedad industrial de algunos fabricantes, así como el temor con base en hechos constatados, de la posibilidad de que esa tecnología disponga de puertas traseras que permitan acciones no deseadas sobre sistemas integrados en infraestructuras relevantes para la seguridad nacional. Dado que cabe la sospecha de que algunas de esas prevenciones sean reforzadas por razones comerciales o económicas, no se puede por menos que insistir en la necesidad de que los Estados estén presentes a la hora de determinar cuáles son los estándares y los requisitos a cumplir a la hora de asegurar ese nivel adecuado de ciberseguridad.

[5] "Measuring the Information Society Report 2018", vol 1, International Telecommunication Unit, 2018, https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf.

En este sentido es especialmente útil la realización de auditorías de ciberseguridad sobre todos los nuevos elementos que se incorporen a las redes, los cuales han de estar libres de toda sospecha tras el correspondiente examen, análisis y certificación en su caso por autoridades públicas competentes en la materia. Esa tecnología, venga de donde venga, que se va a emplear por las empresas privadas a la hora de desplegar esas redes 5G, debe ser fiable en la medida de lo posible. Es necesario insistir en que las autoridades públicas de los Estados deben controlar la tecnología que se va a utilizar para ese despliegue de las nuevas redes 5G, ya que son las responsables últimas de conseguir un adecuado nivel de ciberseguridad que proteja los derechos y libertades de sus ciudadanos frente a riesgos o intromisiones procedentes de esas tecnologías, que ya forman parte de nuestras vidas de un modo impredecible hace tan sólo unos años. Los Estados nacen hace 500 años precisamente para eso, para garantizar un determinado nivel de seguridad en el desenvolvimiento de la vida de sus nacionales. Esa tarea reviste hoy de manera muy notoria perfiles tecnológicos, ya que es en ese quinto dominio, el ciberespacio, donde se ciernen las principales amenazas.