Seguridad en Redes 5G: la acción de la Unión Europea

Margarita Robles Carrillo
Network Engineering and Security Group (NESG)
Universidad de Granada
mrobles@ugr.es

***Resumen*—La seguridad de las redes 5G constituye una preocupación común y compartida por Estados, organizaciones, operadores y proveedores de servicios, empresas y usuarios. La tecnología 5G plantea una problemática compleja porque, más allá de su vertiente técnica, se ha convertido en un asunto de política internacional y en un problema de seguridad. La situación dentro de la Unión Europea (UE) es especialmente complicada porque se trata de un ámbito donde pueden actuar tanto la propia Unión como sus Estados miembros. Mientras estos han empezado a adoptar medidas basadas en razones de interés nacional o seguridad, la UE ha reconocido que la seguridad de las redes 5G es un asunto de importancia estratégica que requiere adoptar un enfoque común europeo. Para ello hay que conciliar los poderes estatales y las competencias de la UE. Esa necesidad es tan evidente como la certeza de que ningún Estado individualmente está capacitado para responder al desafío global que implica la seguridad de las redes 5G.**

***Index Terms*—Redes 5G, Seguridad, Unión Europea, Políticas**

I. Introducción

La seguridad en redes 5G se ha convertido en los últimos tiempos en un problema de naturaleza poliédrica que parece ir más allá de su objeto y alcance natural, esencialmente tecnológico, para manifestarse como un asunto de política, estrategia y seguridad internacional. Las ventajas de esta tecnología se concretan en mayores velocidades y mayor capacidad, latencia, fiabilidad, flexibilidad y eficiencia [1]. Pero también encierra importantes amenazas y riesgos. En la doctrina se ha advertido sobre las principales vulnerabilidades que entraña esta tecnología [2], así como sobre la necesidad de arbitrar soluciones innovadoras en materia de seguridad 5G [3]. Los estudios realizados al respecto por ENISA, la UIT y la ICANN ofrecen un panorama tan estimulante y exhaustivo como inquietante [4].

Más allá de los aspectos tecnológicos, esta tecnología no solo constituye el nuevo paradigma de las comunicaciones electrónicas, sino que, como se reconoce en la normativa española, el 5G es "el componente tecnológico esencial en la transformación digital de la sociedad y de la economía en los países más avanzados durante la próxima década" [5]. A diferencia de lo ocurrido con la sustitución del 3G por el 4G, hay un reconocimiento generalizado del efecto transversal del 5G en el conjunto de la economía y sociedad [6].

Junto con ello, el debate sobre las redes 5G se ha visto en buena medida monopolizado por el discurso adoptado por la Administración Trump contra determinadas empresas vinculadas a China en un contexto internacional marcado por una creciente dependencia tecnológica del país asiático. En 2019, la *National Defense Authorization Act* excluye de los equipamientos de defensa la tecnología desarrollada por empresas extranjeras. En marzo de 2020, la *National Strategy to Secure 5G* confirma su calificación como un asunto de seguridad nacional. Este tipo de acciones se ha considerado como un uso ofensivo del llamado *lawfare* por parte de EEUU contra China. En cualquier caso, el componente de fondo de la guerra comercial, que intermitentemente se reactiva entre estos Estados, no alcanza a explicar la relevancia que han adquirido las redes 5G dentro del discurso político y estratégico. Prueba de ello es la adopción, también, de medidas específicas en otros países. Reino Unido, Alemania, Suecia e Italia han entrado en esa dinámica, aunque destaca, particularmente, el caso de Francia.

El 1 de agosto de 2019 se adoptaba en Francia la Ley nº 2019-810 en cuyo título se advierte claramente su objetivo: "préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles" [7]. Conocida coloquialmente como ley anti-Huawei, esta norma establece un régimen de autorización previa del Primer Ministro para la explotación y funcionamiento de esos equipos y redes. El objetivo expreso de esta medida es salvaguardar los intereses de defensa y seguridad nacional. En febrero de 2021, el Consejo Constitucional ha declarado, por ese motivo, su constitucionalidad. A pesar de tener ese fundamento jurídico que es legítimo, este régimen de autorización previa podría colisionar con la normativa de la UE, en particular, en materia de liberalización del mercado de comunicaciones electrónicas. La UE ha admitido que el despliegue y la gestión de las redes 5G es una cuestión de seguridad nacional. Pero ha reconocido también, precisamente en la Comunicación de la Comisión "UE-China-Una perspectiva estratégica", que la seguridad de las redes 5G es fundamental para garantizar la autonomía estratégica de la Unión [8].

La seguridad 5G no solo es un asunto esencial para los Estados y para la UE, sino que también es un ámbito en el que se concitan competencias nacionales y europeas de manera que no siempre resulta fácil determinar las atribuciones respectivas y la autoridad responsable en última instancia. Hay dos problemas adicionales: por una parte, la seguridad 5G afecta a diversos ámbitos principales de acción de la UE por lo que provoca, si no existe una política común, el riesgo de fragmentación del mercado interior y con ello de los fundamentos mismos de la construcción europea; y, por otra parte, la seguridad 5G plantea un problema de dependencia tecnológica que difícilmente puede ser abordado mediante la acción individual de los Estados. Todo ello apunta a la necesidad de una política efectiva a nivel europeo.

El objeto de este trabajo es analizar el marco jurídico y

operativo de actuación de la UE en materia de seguridad de redes 5G. Para ello, en primer lugar, se considera la normativa existente sobre la que se articula este modelo (Sección II). En segundo término, se analiza el proceso de construcción de la política europea (Sección III). En tercer y cuarto lugar se explican los mecanismos arbitrados con esa finalidad: la evaluación de riesgos (Sección IV) y el denominado *Toolbox on 5G Cybersecurity* (Sección V).

II. El Marco Normativo Europeo

La UE es una organización internacional con competencias atribuidas por los Estados que son los titulares de las mismas. Esto significa que no tiene poderes absolutos o ilimitados sino solo aquellos que se le otorgan en las disposiciones de los Tratados. El resultado es que existe un reparto de poderes entre la UE y los Estados miembros distinto según las materias. La seguridad en redes 5G no está definida como una competencia de la UE en los Tratados, pero hay un marco jurídico que permite actuar en este ámbito.

El análisis de las disposiciones de los Tratados y de los actos adoptados en aplicación de los mismos, en este ámbito concreto, permite afirmar que la política europea en materia de seguridad de redes 5G es el resultado de la combinación de tres pilares normativos: 1) El régimen jurídico de las comunicaciones electrónicas; 2) Las disposiciones sobre seguridad de redes y sistemas de información; y 3) La denominada *Cybersecurity Act* con la que se designa el Reglamento (UE) 2019/881. Este conjunto de normas fundamenta la acción de la UE sobre seguridad 5G, pero cada uno de esos pilares plantea una problemática propia.

1) El régimen jurídico de las comunicaciones electrónicas está actualmente recogido en la Directiva (UE) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (CECE), que debía ser transpuesta por los Estados antes del 21 de diciembre de 2020 [9].

Desde la perspectiva de la organización de la seguridad 5G, este régimen jurídico plantea dos problemas. El primero es la utilización misma de la directiva como instrumento regulador que, a diferencia del reglamento, deja un amplio margen de actuación a los Estados y, sobre todo, implica que los derechos y obligaciones para empresas y usuarios derivan de la norma interna de transposición -y no directamente de la europea- que puede marcar diferencias en cuanto a la regulación entre los distintos Estados miembros. El segundo problema se encuentra en el hecho de que, en febrero de 2021, la mayoría de los Estados aún no habían transpuesto la directiva. Ello genera una considerable inseguridad jurídica en un momento clave para la seguridad 5G.

2) La normativa adoptada en el marco de la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y de los sistemas de información [10], conocida como Directiva NIS, establece un régimen jurídico que se aplica a operadores de servicios esenciales y proveedores de servicios digitales centrado en los requisitos de seguridad y de notificación de incidentes. La invocación de esta normativa en materia de seguridad 5G plantea dos problemas. El primero es que ya se encuentra en marcha el proceso de revisión de la Directiva NIS, abundando con ello en la incertidumbre normativa que también se plantea en materia de comunicaciones electrónicas. El segundo es que la propia Directiva NIS establece, en su artículo 1.3, que las disposiciones previstas en ella no serán aplicables a las empresas sometidas al régimen de comunicaciones electrónicas.

Aplicar los requisitos de la Directiva NIS a las comunicaciones electrónicas, cuando la propia directiva excluye expresamente esa posibilidad, es un problema jurídico grave. Una posible solución sería aprovechar la reforma prevista de la Directiva NIS para resolver esta situación.

3) La *Cybersecurity Act* [11] tiene dos partes diferenciadas: las normas sobre ENISA, que se designa como Agencia de la UE para la Ciberseguridad, y la normativa sobre el marco europeo de certificación de la ciberseguridad. Siendo avances significativos, hay dos puntos débiles en esta regulación: su naturaleza progresiva y su carácter voluntario, que no permiten vislumbrar una solución a corto plazo en materia de homogeneidad de la certificación europea.

En realidad, dentro de este tríptico normativo, el marco jurídico más sólido es la Directiva CECE que aún no ha sido transpuesta en muchos países incluida España. El CECE establece que los Estados miembros velarán por que los proveedores de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles al público adopten las medidas técnicas y organizativas adecuadas y proporcionadas para gestionar adecuadamente los riesgos existentes para la seguridad de sus redes y servicios (artículo 40). Aunque algunas de las medidas son similares, no son iguales a las previstas en la esfera NIS. Basta comprobar los parámetros para la determinación de la importancia de un incidente de seguridad recogidos en el artículo 40.2 de la Directiva CECE con los establecidos en el artículo 14.4 de la Directiva NIS. La aplicación y el control del cumplimiento de ambos regímenes normativos son similares, pero más estrictos en el CECE.

En definitiva, este marco normativo europeo resulta, innecesariamente, incoherente y complejo. No obstante, y a pesar de ello, ha posibilitado la construcción de un enfoque europeo sobre seguridad 5G.

III. El Proceso de Construcción de un Enfoque Europeo

Aunque hubo algunas iniciativas previas, el Plan de Acción 5G para Europa presentado en una Comunicación de la Comisión, en septiembre de 2016, constituye el punto de partida efectivo de esta acción europea [12]. El problema principal que plantea este informe en materia de seguridad 5G es el riesgo de fragmentación en términos de disponibilidad de espectro, continuidad del servicio a través de las fronteras y aplicación de las normas como consecuencia de la falta de coordinación de los enfoques nacionales.

El Plan de Acción persigue una coordinación adecuada a nivel europeo basada en una serie de pilares: 1) Un calendario común para la implantación del 5G; 2) La eliminación de los obstáculos para ampliar y facilitar el espectro radioeléctrico de 5G; 3) La multiplicación de las conexiones fijas e inalámbricas; 4) La preservación de la interoperabilidad global; y 5) La innovación 5G para apoyar el crecimiento. Como expresamente advierte, este Plan adopta un enfoque ambicioso pero se trata de un documento de la Comisión,

y no del conjunto de las instituciones, que no tiene carácter vinculante desde el punto de vista jurídico.

La posibilidad de actuar con una norma más efectiva, jurídicamente vinculante, a nivel europeo parece complicada. Por una parte, las otras instituciones principales de la UE se han limitado a regular aspectos concretos, como ocurre con la Decisión (UE) del Parlamento Europeo y del Consejo, de 17 de mayo de 2017, sobre el uso de la banda de frecuencia 470-970 MHz. En esta declaración se reconoce expresamente que las redes 5G tendrán importantes repercusiones no solo para el sector digital, sino para las economías en su conjunto y que el lanzamiento con éxito del 5G será crucial para el desarrollo económico y para la competitividad y la productividad de las economías de la Unión [13]. A pesar de esta afirmación, no parece existir la voluntad política necesaria para aprobar medidas jurídicas vinculantes a nivel europeo.

Esa conclusión se confirma cuando los Estados miembros de la UE adoptan, el 18 de julio de 2017, la *Declaración Ministerial de Tallin* sobre 5G [14]. El hecho de pronunciarse mediante una declaración ministerial -y no a través de un acto o de unas conclusiones del Consejo- tiene importantes consecuencias jurídicas y políticas. La elección de este instrumento normativo constituye una afirmación de su propia y principal responsabilidad nacional y una consecuente limitación de la capacidad de acción de la UE, cuando podría haberse hecho a la inversa. Implica limitar la acción de la UE a una función de coordinación de acciones y políticas nacionales en materia de seguridad 5G. Esta decisión puede resultar discutible porque, en buena lógica, una política común europea resultaría más competitiva y más efectiva a nivel mundial que las acciones individuales nacionales.

No obstante, pese a ello, la Declaración de Tallin ha de ser valorada positivamente en la medida en que expresa un cierto consenso de los Estados miembros en materia de seguridad 5G. Ese consenso abarca tres ámbitos de acción. En primer lugar, los principios básicos son: 1) Aumentar la disponibilidad del espectro radioeléctrico; 2) Fortalecer los principios básicos de la gestión racional del espectro, principalmente, el acceso no discriminatorio al espectro radioeléctrico; y 3) Garantizar la cobertura y la conectividad. En segundo término, se adoptan dos modalidades principales de medidas de carácter operativo: por un lado, facilitar el despliegue de la fibra óptica para aprovechar el potencial de las redes 5G; y, por otro, apoyar la implementación de células pequeñas considerando que el uso integral de 5G requiere una densificación en términos de estaciones base en las diferentes gamas del espectro radioeléctrico. Por último, se establecen dos parámetros de comportamiento: por una parte, preservar la interoperabilidad mundial del 5G mediante un enfoque integral e inclusivo como una prioridad para el Mercado Único Digital; y, por otra, establecer un diálogo estratégico que podría extenderse al conjunto de la comunidad *multi-stakeholder*, incluyendo promover a los pioneros y apoyar el aprendizaje entre pares y la transparencia.

Esta línea de actuación, que reconoce la responsabilidad principal de los Estados, no supone excluir una acción europea sino limitar el alcance de dicha acción: la UE solo tiene asignada una función de apoyo, fomento o complemento de las medidas de los Estados miembros. En el ejercicio de esa función, en marzo de 2019, el Consejo Europeo solicita a la Comisión una propuesta sobre un planteamiento concertado en materia de seguridad de redes 5G [15] que se materializa en la *Recomendación (UE) 2019/534, de 26 de marzo de 2019, sobre la Ciberseguridad de las redes 5G* [16].

Son tres las aportaciones principales de la Recomendación 2019/534 de la Comisión. La primera es que refuerza la competencia europea en materia de seguridad 5G al reconocer que esa tecnología constituye una prioridad dentro de la Estrategia para el Mercado Único Digital porque es la espina dorsal de una amplia gama de servicios esenciales para el funcionamiento del mercado interior y el mantenimiento de funciones sociales y económicas vitales. La necesidad de adoptar medidas para mantener un elevado nivel común de seguridad en las redes 5G se justifica por la propia existencia del mercado interior, unida a la naturaleza interconectada y transnacional del ecosistema digital que implica que cualquier incidencia o vulnerabilidad en un Estado miembro podría afectar a la UE en su conjunto.

Una segunda contribución especialmente destacable de esta Recomendación es que procede a una definición integral y global de las redes 5G entendidas como "el conjunto de todos los elementos de la infraestructura de red pertinentes para las tecnologías de las comunicaciones móviles e inalámbricas utilizados en los servicios de conectividad y de valor añadido con características de alto rendimiento, tales como capacidades y velocidades de datos muy elevadas, comunicaciones de baja latencia, fiabilidad ultra-elevada o soporte de un elevado número de dispositivos conectados".

La tercera aportación de este acto de la Comisión se encuentra en el establecimiento de los objetivos, las medidas y el procedimiento para organizar la seguridad de las redes 5G. Una primera etapa se centra en una acción a nivel nacional mediante la evaluación de riesgos de la infraestructura 5G por parte de los Estados y la revisión de los requisitos de seguridad y de los medios de gestión de riesgos teniendo en cuenta tanto factores técnicos como de otra índole. La segunda fase consiste en una acción coordinada a nivel de la UE con un doble objetivo: realizar una evaluación coordinada de los riesgos y adoptar un conjunto de herramientas comunes para hacer frente a los mismos.

La Recomendación 2019/534 de la Comisión recibe el apoyo explícito del Consejo de la UE, el 3 de diciembre de 2019, en sus *Conclusiones sobre la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G* [17]. En ellas, además, el Consejo realiza dos aportaciones principales. Por una parte, reconoce que la introducción rápida y segura de las redes 5G es fundamental para mejorar la competitividad de la UE y requiere un planteamiento coordinado em la UE, sin perjuicio de las competencias de los Estados miembros. Por otra parte, incide en un aspecto fundamental -y novedoso respecto de los actos anteriores- al afirmar que "la generación de confianza en las tecnologías 5G está firmemente enraizada en los valores fundamentales de la UE –como los derechos humanos y las libertades fundamentales, el Estado de Derecho y la protección de la intimidad, los datos personales y la propiedad intelectual–, en el compromiso con la transparencia, la fiabilidad y la inclusión de todas las partes interesadas y

todos los ciudadanos".

Con este apoyo del Consejo y, por tanto, de los Estados miembros, se pone en marcha el operativo diseñado en la Recomendación 2019/534. En julio de 2019, las evaluaciones nacionales son enviadas a la Comisión y a ENISA con la finalidad de constituir, junto con el informe técnico de este órganismo, el fundamento para una evaluación coordinada de los riesgos de la UE, que es aprobada el 9 de octubre de 2019 (IV). Esta evaluación es, a su vez, la base para la elaboración del *EU Toolbox on 5G Cybersecurity* que es adoptado el 29 de enero de 2020 (V).

IV. Evaluación Coordinada de Riesgos (EURAC5G)

El EURAC5G es definido como un informe de alto nivel acordado por los Estados, con el apoyo de la Comisión y de ENISA, donde se exponen las principales conclusiones comunes resultantes de las evaluaciones nacionales de riesgos sobre las redes 5G [18]. No se trata de un estudio exhaustivo, sino que está centrado en los elementos de importancia estratégica para la UE. Constituye, según sus términos, el primer paso de un proceso dirigido a garantizar la seguridad sólida y a largo plazo de las redes de 5G. No es texto jurídico, pero refleja un consenso básico que puede marcar el camino hacia un mayor grado de compromiso.

El EURAC5G asume la definición de redes 5G realizada en la Recomendación 2019/534, identificando tres de sus características técnicas que constituyen una diferencia sustantiva respecto de la situación previa, a saber: 1) El movimiento hacia el software y la virtualización a través de tecnologías como el *Software Defined Network* (SDN) y la *Network Functions Virtualisation* (NFV); 2) El desarrollo del *Network Slicing*; y 3) Una mayor funcionalidad en los extremos de la red y una arquitectura menos centralizada. En términos de seguridad, supone un aumento de la complejidad de la cadena de suministro, un incremento de la dependencia de los operadores de red respecto de terceros proveedores y, en consecuencia, una mayor complejidad en la distribución de responsabilidades entre los distintos implicados. A ello hay que sumar una previsible extensión de la superficie de ataque y del número de posibles entradas para el atacante.

Una vez definido este marco general, el EURAC5G sigue la metodología de evaluación de riesgos de la ISO/IEC 27005 [19]. Esa evaluación abarca los siguientes elementos: amenazas, actores, activos, vulnerabilidades, riesgos y escenarios relacionados.

Las principales *amenazas* son aquellas relacionadas con la confidencialidad, la disponibilidad y la integridad. Entre ellas se incluye la disrupción local o global de las redes 5G, el espionaje, la modificación o el re-direccionamiento del tráfico o de los datos o la destrucción o la alteración de otras infraestructuras o sistemas a través de las redes 5G.

Los *actores* son clasificados en diversas categorías: accidentales/no adversarios, hackers individuales (definidos erróneamente como criminales aficionados o lobbistas), grupos activistas, *insiders*, agentes estatales y otros posibles actores desde corporaciones a ciberterroristas.

Los *activos* se evalúan categorizando componentes lógicos y funcionales donde se incluyen las funciones básicas y de acceso definidas en la 3GPP (*3rd Generation Partnership Project*) y las funciones subyacentes, no definidas en ella, de transporte y transmisión, intercambio de redes y sistemas de gestión y servicios de apoyo.

Las *vulnerabilidades* se clasifican en varias categorías distinguiendo entre aquellas relacionadas con el hardware, el software, los procesos y políticas y las de los proveedores.

Los *escenarios de riesgo* son identificados distinguiendo entre los siguientes: 1) Los derivados de medidas insuficientes de seguridad, como una mala configuración de las redes o la falta de controles de acceso; 2) Los relacionados con la cadena de suministros 5G, como los fallos o vulnerabilidades de los equipos o la propia dependencia de un solo proveedor; 3) Los procedentes del *modus operandi* de los autores de las amenazas; 4) Los resultantes de la interdependencia entre las redes 5G y otros sistemas críticos; y 5) Los provocados por los dispositivos de los usuarios.

El EURAC5G reconoce expresamente que la tecnología 5G crea un nuevo paradigma de seguridad que exige reevaluar el marco normativo actual. Con el objetivo de responder a los desafíos planteados en el EURAC5G, el 29 de enero de 2020, se adopta el EU *Toolbox on 5G Cybersecurity*.

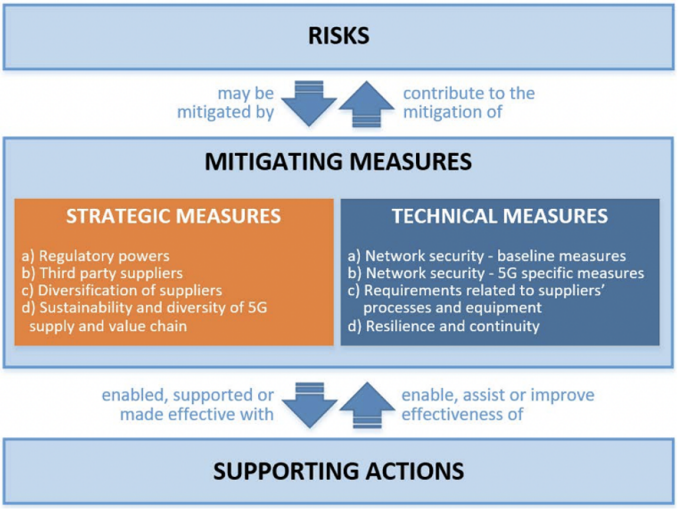
V. EU TOOLBOX ON 5G CYBERSECURITY (EUT5G)

El EUT5G parte de un principio básico: la seguridad de las redes 5G es esencial para proteger las economías y sociedades y para garantizar la soberanía tecnológica de la Unión [20]. El objetivo principal del EUT5G es definir un enfoque coordinado europeo basado en la seguridad y el riesgo que sea compatible con el mercado interior.

El EUT5G es un sistema establecido en un documento acordado dentro del Grupo de Cooperación creado en el marco de la Directiva NIS donde están representados los Estados, la Comisión y la Agencia Europea de Ciberseguridad. Desde la perspectiva de su *naturaleza*, no es un texto jurídicamente vinculante. Como se reconoce expresamente, solo traslada el sólido compromiso de los Estados y la Comisión de usar y aplicar las medidas recomendadas siguiendo la metodología prevista para hacer frente a los riesgos identificados en el EURAC5G.

Siguiendo el *modelo de delimitación de competencias* recogido en el EUT5G, los Estados son responsables principales con las siguientes atribuciones: 1) Reforzar los requisitos de seguridad para los operadores de redes móviles; 2) Evaluar el perfil de riesgo de los proveedores; y 3) Establecer una estrategia de proveedores dirigida a garantizar un equilibrio adecuado de proveedores a nivel nacional, evitar o limitar la dependencia de un solo proveedor o de proveedores de alto riesgo y asegurar que cada operador tenga, a su vez, una estrategia de múltiples proveedores. La Comisión, junto con los Estados, tiene asignadas dos funciones principales: 1) Facilitar la coordinación entre ellos en materia de normalización y certificación; y 2) Promover una cadena de suministro 5G diversa y sostenible para evitar la dependencia a largo plazo aprovechando los instrumentos existentes y fortaleciendo las capacidades de la UE en 5G con programas y financiación.

El EUT5G establece tres tipos de *medidas*: estratégicas, técnicas y de apoyo. Los *planes de mitigación de riesgos* han de consistir en combinaciones posibles de esta tipología de medidas en función de la naturaleza y el alcance del riesgo,



que puede ser calificado como muy alto, alto, medio o bajo. Las medidas se adoptarán por las autoridades nacionales o europeas. Siguiendo la tabla diseñada en el EUT5G, la figura *supra* muestra el modelo operativo.

En julio de 2020, se publica el informe sobre la implementación por parte de los Estados del EUT5G y en septiembre la Comisión adopta la Recomendación C (2020), 6270 final, sobre un conjunto de herramientas comunes de la Unión para reducir el costo del despliegue de redes de muy alta capacidad y garantizar un acceso oportuno y favorable a la inversión al espectro radioeléctrico de 5G, a fin de fomentar la conectividad en apoyo de la recuperación económica de la crisis de COVID-19.

VI. Conclusiones

La tecnología 5G se ha definido como un componente clave para el desarrollo de la economía y de la sociedad en su conjunto. Por ello y por tratarse de una tecnología que no se encuentra al alcance de todos los Estados, ni de todos los operadores y proveedores de servicios, se ha convertido en un bien y en un servicio de valor estratégico que permite visualizar en términos prácticos y apreciar efectivamente el alcance del problema de la dependencia o, incluso, de la brecha tecnológica entre los distintos países y operadores. Las actuaciones contra personas o intereses chinos o las presiones a sus homólogos occidentales por parte de EEUU muestran que el debate sobre las redes 5G se ha convertido en un asunto prioritario en el marco de la política internacional, que ha llegado a calificarse como problema de seguridad internacional con todo lo que ello implica desde una perspectiva jurídico-política. La adopción de medidas nacionales, como en el caso de Francia, Suecia o Italia, destinadas a preservar los intereses de la seguridad y la defensa nacional es una evidencia más de la naturaleza no exclusivamente técnica de la seguridad de las redes 5G. Pero, precisamente porque es un problema más grave y complejo, una acción nacional puede resultar insuficiente e injustificada cuando existe una organización internacional como la UE que puede ofrecer una respuesta más efectiva y más amplia.

La UE reconoce la existencia de un problema y de un interés de seguridad nacional de los Estados y, también, el valor estratégico de la seguridad 5G para el conjunto de la Unión. Pero, la UE es un actor singular que se encuentra en una posición especial por varios motivos. Como primera providencia, la UE no es un Estado con la plenitud, integridad y exclusividad de las competencias para gestionar la seguridad de las redes 5G como pueden hacerlo EEUU, China o el resto de los países del mundo. La UE es una organización internacional que solo cuenta con las competencias que le atribuyen sus países miembros y que, incluso dentro de sus ámbitos de competencia, actúa a través de los propios Estados y en cooperación o coordinación con ellos.

Como consecuencia de ello, en el ámbito europeo, la seguridad 5G se sitúa en una encrucijada por la combinación de una triple circunstancia: a) Es una cuestión de seguridad nacional para los Estados, que se encuentra en su esfera de competencia; b) Es un componente básico del mercado interior y de la estructura de la sociedad y de la economía del conocimiento, que forman parte de las competencias de la UE; y c) Ningún Estado individualmente cuenta con la capacidad y los medios, a corto o medio plazo, para garantizar esa seguridad, mientras que la UE carece de la competencia principal para abordar esa cuestión en su conjunto. La tecnología 5G está potencialmente llamada a afectar a cualquier ámbito de actividad, circunstancia que complica extraordinariamente su articulación normativa y funcional.

A diferencia del resto de los Estados de la sociedad internacional, que mantienen la totalidad de sus prerrogativas para gestionar esta y otras tecnologías, en el ámbito de la UE, la seguridad 5G requieren un ejercicio combinado de los poderes de los Estados y de las competencias atribuidas a la UE. La opción por un modelo coordinado articulado sobre la base de medidas de *soft law* y dirigido a establecer un enfoque europeo se ha convertido en la única alternativa posible en el estado actual de reparto de competencias entre la Unión y sus miembros. Este enfoque se ha concretado en medidas como el EURAC5G y el EUT5G.

El EUT5G supone el establecimiento de un conjunto de medidas que tiene como destinatarios a los Estados y de acciones encomendadas a la Comisión para ser realizadas en cooperación/coordinación con los Estados. La explicación que se ha realizado de este mecanismo es suficiente para apreciar que no se ha atribuido a la UE una competencia principal en materia de seguridad de redes 5G que permita la articulación de una política común europea. Manteniéndose los Estados como principales titulares y responsables de la misma, la función de la UE consiste en procurar la generación de un enfoque europeo basada en la coordinación de las políticas nacionales y el impulso de la Unión.

En definitiva, el análisis de las medidas adoptadas en el marco de la UE en materia de seguridad de las redes 5G pone de manifiesto que las competencias y la acción de la UE son limitadas por tratarse de una responsabilidad principal de los Estados miembros. Pero, las propias limitaciones de estos países en el marco de esa tecnología, junto con el hecho de que hay que combinar sus atribuciones con las de la UE en el marco del mercado único, constituyen un obstáculo al desarrollo de políticas efectivas de seguridad de las redes 5G.

La dependencia tecnológica que impone la tecnología 5G es un hecho que solo se puede abordar con ciertas garantías

de efectividad con una acción a nivel europeo. Ningún Estado miembro cuenta con la capacidad para superar esa situación que tampoco sería factible dentro del propio mercado único digital que no posibilita políticas nacionales autónomas. Esa situación solo se puede revertir con una política europea que, por sus dimensiones y sus componentes, podría constituir una alternativa a la preeminencia de empresas procedentes o avaladas por otros países, particularmente, China. Un consorcio de empresas europeas, con una fuerte financiación europea o incluso con una participación pública, justificada por la naturaleza de bien o servicio público que habría de recibir el despliegue y el funcionamiento de las redes 5G, podría ser la solución frente a la dependencia externa. El apoyo de los agentes económicos a una política europea ya se hizo público en diciembre de 2019 en una Declaración de los CEOs de las principales operadores y proveedores de servicios de telecomunicaciones sobre el propósito de las redes digitales [21]. El EURAC5G y el EUT5G son un primer paso en esa dirección, pero es necesario un impulso más efectivo y un mayor compromiso para construir una política europea capaz de garantizar la ciberseguridad de las redes 5G.

En España, a finales de 2020, se ha presentado para audiencia pública el Anteproyecto de Ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas 5G siguiendo las directrices marcadas por la UE [22]. Esta norma se adopta en cumplimiento de la Recomendación 2019/534 de la Comisión, así como del resto de las medidas adoptadas a nivel europeo. Los objetivos principales son: 1. Reforzar la seguridad en la operación de las redes 5G y en las prestaciones de servicios; 2. Promover un mercado de suministradores suficientemente diversificado y evitar la dependencia de suministradores con una calificación de riesgo elevado; 3. Evitar posibles injerencias de terceros actores en la cadena de suministro; 4. Fortalecer la industria y fomentar la I+D+i nacionales; y 5. Proteger la seguridad nacional. El proyecto incluye un capítulo sobre análisis y gestión de riesgos, establece un esquema de seguridad de las redes y servicios 5G y define las potestades administrativas de control y sanción. El Ministerio de Asuntos Económicos y Transformación Digital centraliza las competencias en la materia en la que también se prevé la intervención a título consultivo del Consejo de Seguridad Nacional. Según su propio enunciado, esta ley se dicta para garantizar un bien de interés general, como es la seguridad y confianza en las comunicaciones electrónicas.

Agradecimientos

Este trabajo ha sido financiado por el Gobierno de España, con fondos FEDER, a través del proyecto TIN2017-83494-R y del Proyecto EQC2019-005605-P MAstering 5G: deep learninG and smart Infrastructure Communications for a secure connected society (MAGIC-5G).

Referencias

[1] UIT.*Sentando las bases para la 5G: oportunidades y desafíos*, 2018.

[2] J. G. Andrews et al., "What Will 5G Be?", *IEEE Journal on Selected Areas in Communications*, vol. 32, n. 6, pp. 1065-1082, 2014; F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta y P. Popovski, "Five disruptive technology directions for 5G", *IEEE Communications Magazine*, vol. 52, n. 2, pp. 74-80, 2014.

[3] M. Gil Pérez, A. Huertas Celdrán, F. Ippoliti, M. Zago, V. M. Ruiz Sánchez, A. Hernández Chillón, F.J. García Clemente, L. Fernández Maimó, D. Sevilla Ruiz y G. Martínez Pérez. "Despliegue automático de aplicaciones NFV y SDN para detectar y mitigar ciberamenazas en redes 5G", en *Actas de las III Jornadas Nacionales de Investigación en Ciberseguridad*, Universidad Rey Juan Carlos, Madrid, pp. 59, 2017; S.R. Husain, M. Echeverria, I, Karim, O, Chowdhury y E. Bertino. "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol", *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 669-684, 2019.

[4] ENISA. *Threat Landscape for 5G Networks*, 2019 (https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks); UIT *Sentando las bases para la 5G: Oportunidades y desafíos*, 2018; ICANN *Tecnología 5G*, Oficina del Director de Tecnologías, 2020. Pueden verse las propuestas de la Conferencia de Praga (https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/).

[5] Orden ECE/1016/2018, de 28 de septiembre, por la que se establecen las bases reguladoras de la concesión de subvenciones a proyectos piloto de tecnología 5G. BOE, nº 239, de 3 de octubre de 2018, p. 96384.

[6] Ministerio de Energía, Turismo y Agenda Digital. *Plan Nacional 5G (2018-2020)*. El Plan Nacional 5G adoptado por España a finales de 2017, que se ha estructurado en cuatro ejes de actuación: Gestión y planificación del espacio radioeléctrico; Impulso a la tecnología 5G; Aspectos regulatorios; Coordinación y cooperación internacional (https://avancedigital.gob.es/5G/Documents/plan_nacional_5g.pdf).

[7] https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038864094.

[8] Comisión Europea. *Comunicación Conjunta al Parlamento Europeo, el Consejo Europeo y el Consejo "UE-China - Una perspectiva estratégica"*, JOIN (2019) 5 final, de 12 de marzo de 2019.

[9] DOUE, L 321, de 17.12.2018, pp. 36 y ss.

[10] DOUE, L 194, de 19.07.2016, pp. 1 y ss.

[11] DOUE, L 151, de 07.06.2019, pp. 15 y ss.

[12] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0588&from=es.

[13] DOUE, L 138, de 25.05.2017, pp. 131-132.

[14] https://mmpi.gov.hr/UserDocsImages/arhiva/Ministerial-declaration-5G-final-signed.pdf.

[15] https://www.consilium.europa.eu/es/press/press-releases/2019/03/22/european-council-conclusions-22-march-2019/.

[16] DOUE, L 88, de 29.03.2019, p. 42.

[17] Consejo de la Unión Europea. *Conclusiones de 3 de diciembre de 2019 sobre la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G* (https://www.consilium.europa.eu/media/41595/st14517-en19.pdf).

[18] NIS Cooperation Group. *EU Coordinated Risk Assessment of the Cybersecurity of 5G networks*, 2019 (https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf).

[19] https://www.iso27001security.com/html/27005.html.

[20] NIS Cooperation Group. *Cibersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*, 2020 (https://www.politico.eu/wp-content/uploads/2020/01/POLITICO-Cybersecurity-of-5G-networks-EU-Toolbox-January-29-2020.pdf).

[21] https://etno.eu/news/all-news/655-ceos-statement-digital-networks.html.

[22] https://avancedigital.mineco.gob.es/es-es/Participacion/Documents/5G_audiencia/Texto_APL_ciberseguridad_5G.pdf?csf=1&e=48JHOH.