MEMORIA DE ANÁLISIS DE IMPACTO NORMATIVO DEL ANTEPROYECTO DE LEY SOBRE REQUISITOS PARA GARANTIZAR LA SEGURIDAD DE LAS REDES Y SERVICIOS DE COMUNICACIONES ELECTRÓNICAS DE QUINTA GENERACIÓN.

RESUMEN EJECUTIVO

Ministerio/Órgano proponente	Ministerio de Asuntos Económicos y Transformación Digital Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales	Fecha	9 de diciembre de 2020
Título de la norma	Ley…/…. sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.		
Tipo de Memoria	Normal ☒ Abreviada ☐		
OPORTUNIDAD DE LA PROPUESTA			
Situación que se regula	Las medidas que deben adoptarse para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas basadas en la tecnología 5G.		
Objetivos que se persiguen	Desarrollar un entorno confiable para el desarrollo y adopción de las redes y servicios 5G dando garantías a los usuarios de su protección frente a los riesgos que más afectan a estas redes y servicios, como son los derivados de su conectividad masiva y de la dependencia de un número limitado de suministradores para la operación de la red.		
Principales alternativas consideradas	• No hacer nada y seguir aplicando el artículo 44 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. • Animar a los operadores y prestadores de servicios a aplicar la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre la ciberseguridad de las redes 5G, el análisis de		

	riesgos coordinado de los Estados miembros y la "caja de herramientas" acordada por éstos en desarrollo de la Recomendación. • Aprobar mediante Real Decreto u Orden ministerial normas o instrucciones de seguridad para las redes y servicios 5G, al amparo, respectivamente, de la disposición final décima o del artículo 44.4 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
CONTENIDO Y ANÁLISIS JURÍDICO	
Tipo de norma	Norma con rango de ley
Estructura de la Norma	El anteproyecto consta de una Exposición de Motivos, veintidós artículos divididos en cuatro capítulos, dos disposiciones adicionales, una disposición transitoria y tres disposiciones finales.
Informes recabados	El anteproyecto de ley habrá de elevarse al Consejo de Ministros y ser sometido previamente a Dictamen del Consejo de Estado
Trámite de audiencia	El anteproyecto ha sido sometido a trámite de consulta pública previa que finalizó el día 13 de diciembre de 2019. El anteproyecto ha de ser sometido a trámite de audiencia pública.
ANÁLISIS DE IMPACTOS	
Adecuación al orden de competencias	La ley se dicta al amparo de las competencias estatales en materia de telecomunicaciones y de seguridad pública establecidas en los artículos 149.1.21ª y 149.1.29ª de la Constitución.

Impacto económico y presupuestario	Efectos sobre la economía en general	De acuerdo con estudios de la Comisión Europea los beneficios estimados al introducir 5G en cuatro sectores productivos (automoción, salud, transporte y utilities) aumentarían progresivamente hasta alcanzar en 2025 los 62.500 millones de euros de impacto directo anual dentro de la Unión Europea, que se elevarían a 113.000 millones de euros sumando los impactos indirectos. El mismo estudio estima que en nuestro país se obtendrían unos beneficios indirectos en los cuatro sectores analizados de 14.600 millones de euros y una importante creación de empleos. La confianza en la seguridad de las redes y servicios 5G es clave para extender su utilización entre ciudadanos y empresas.
	En relación con la competencia	☐ la norma no tiene efectos significativos sobre la competencia ☒ la norma tiene efectos positivos sobre la competencia. ☐ la norma tiene efectos negativos sobre la competencia
	Desde el punto de vista de las cargas administrativas	☐ supone una reducción de cargas administrativas. ☒ incorpora nuevas cargas administrativas.

		☐ no afecta a las cargas administrativas
	Desde el punto de vista de los presupuestos, la norma: ☐ Afecta a los presupuestos de la Administración del Estado ☐ Afecta a los presupuestos de otras Administraciones Territoriales	☐ implica un gasto ☐ implica un ingreso
Impacto de género	La norma tiene un impacto de género	Negativo ☐ Nulo ☒ Positivo ☐

Otros impactos considerados		-Impacto en la lucha contra la despoblación y el cambio climático. -Impacto en relación con la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas con discapacidad. -Impacto en relación con la infancia la adolescencia y la familia**.**
Otras consideraciones		

A. OPORTUNIDAD DE LA PROPUESTA

1. Motivación.

- Causas:

Como señala la Comunicación de la Comisión Europea, de 14 de septiembre de 2016, "La 5G para Europa: un plan de acción", la tecnología 5G se considera una oportunidad estratégica para Europa, ya que permite transformaciones industriales mediante servicios inalámbricos de banda ancha a velocidades de gigabit, el apoyo de nuevos tipos de aplicaciones que conectan objetos y dispositivos (Internet de las cosas), y la versatilidad de las redes mediante la virtualización del "software", lo que permite modelos empresariales innovadores en numerosos sectores (por ejemplo, transportes, sanidad, industria manufacturera, logística, energía, medios de comunicación y entretenimiento). Su adopción debe ser rápida para que se traduzca en una ganancia de competitividad frente a los gigantes de la economía mundial.

Para ello, la Comisión Europea puso en marcha en 2016 un ambicioso plan de acción que fija como fecha objetivo para su introducción comercial a gran escala 2020. El plan de acción con de enero de templa, entre otras medidas, la realización de pruebas piloto para probar posibles usos de la tecnología 5G y estimular una demanda temprana de servicios. En febrero de 2020, la Comisión Europea adoptó la estrategia para el periodo 2020-25, "Configurando el futuro digital de Europa" donde señala la previsión de una revisión del Plan de Acción 5G para Europa en el año 2021.

De acuerdo con el plan de acción comunitario, en España, mediante Orden ECE/1016/2018, de 28 de septiembre, se establecieron las bases reguladoras de la concesión de subvenciones a proyectos piloto de tecnología 5G. El 30 de abril de 2019 se resolvió la primera convocatoria de pilotos 5G promovida por el Gobierno, a través de Red.es. Se trata de dos pilotos, que contemplan 32 casos de uso en Andalucía y 8 casos de uso en Galicia, focalizados en sectores como servicios de salud, seguridad y emergencias, audiovisual y multimedia, vehículos conectados, agricultura, industria 4.0, turismo, aplicaciones de realidad virtual y aumentada, control de drones, acceso fijo por radio o supervisión de infraestructuras.[1]

Una vez puestos en marchas estos primeros pilotos 5G, La Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G, propuso una acción coordinada de los Estados miembros para analizar los riesgos de seguridad de la tecnología 5G y la recopilación y aplicación de buenas prácticas que garanticen la seguridad de estas redes. Los Estados miembros apoyaron esta Recomendación en las conclusiones acordadas por el Consejo de la Unión Europea de 3 de diciembre de 2019.

El día 29 de enero de 2020, se publicó la "caja de herramientas" o "toolbox" europeo en el que se identifican un conjunto de medidas susceptibles de ser adoptadas por los Estados miembros para mitigar los principales riesgos para la ciberseguridad de las redes 5G y para guiar a los Estados miembros en la selección de las medidas que deben priorizarse en los planes de mitigación de riesgos a nivel estatal y comunitario, de modo que se asegure un adecuado nivel de cirberseguridad de las redes 5G a escala europea y unos criterios coordinados entre Estados miembros.

La Comunicación de la Comisión "Despliegue seguro de la 5G en la UE, de la misma fecha de 29 de enero de 2020 "Aplicación de la caja de herramientas de la UE" señala que las conclusiones y acciones recomendadas en el "toolbox" han de ser "medidas clave" que deben implementar los Estados miembros y la Comisión europea para garantizar la seguridad de estas redes en Europa.

De ambos documentos se desprende que la tecnología 5G supondrá no solo un cambio tecnológico en las redes de comunicaciones móviles, sino que también lo inducirá en el conjunto de la economía y la sociedad.

Para ello es necesario que ciudadanos y empresas perciban que la tecnología 5G es fiable y seguro, de manera que puedan confiar en ella para desarrollar procesos complejos o de gran precisión, sin riesgo de fuga de datos personales o empresariales.

El impacto de un incidente de seguridad en las redes 5G puede trascender el ámbito de las comunicaciones interpersonales y el acceso a Internet (que son las funciones básicas de las actuales redes de comunicaciones móviles) y afectar a distintas actividades económicas y

[1] Posteriormente mediante Acuerdo del Consejo de Ministros de 4 de octubre de 2019 se ha autorizado la realización de un gasto de hasta 45 millones de euros para subvencionar otros 11 proyectos piloto

sociales[2]. En primer lugar, por la alta velocidad, baja latencia y la conectividad masiva que introduce , pero también por el desplazamiento a los bordes de la red de funciones que antes se controlaban desde el centro y por la división de la red en distintas capas o segmentos con diversos grados de seguridad.

Además, la arquitectura de las redes 5G no será tanto física como lógica, por lo que aumentará la dependencia de proveedores de componentes y programas externos y, por tanto, habrá más actores involucrados en su gestión y, por ende, más vectores de ataque.

Por último, las redes 5G se apoyarán inicialmente en las redes 4G existentes y, por tanto, heredarán sus vulnerabilidades.

En definitiva, la motivación de esta norma es permitir el establecimiento de medidas con las que afrontar los riesgos de seguridad a los que están expuestos las nuevas redes y servicios 5G. Cabe señalar, que la normativa es uno de los compromisos incluidos dentro de la estrategia "España Digital 2025" dentro de su eje prioritario de impulso a la tecnología 5G, que

---

[2] Los siguientes documentos ofrecen una visión general de los riesgos de seguridad asociados a la tecnología 5G:

- *EU coordinated risk assessment of the cybersecurity of 5G networks* (Grupo de cooperación de la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión), de 9 de octubre de 2019. Este documento analiza las principales amenazas, los actores que pueden poner en riesgo las redes 5G, sus activos más sensibles y sus puntos débiles, así como situaciones de riesgo que pueden producirse. https://europa.eu/rapid/press-release_IP-19-6049_en.htm
- *ENISA Threat Landscape for 5G networks*, de noviembre de 2019: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks ENISA es la Agencia europea de ciberseguridad.
- *Overview of risks introduced by 5G adoption in the United States* (Agencia estadounidense de ciberseguridad y seguridad de las infraestructuras), de julio de 2019: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf
- *UK Telecoms supply chain overview report* (Ministerio de digitalización, cultura, medios de comunicación y deporte del Reino Unido), de julio de 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf
- *Summary of NCSC's security analysis for the UK telecoms sector* (Centro de ciberseguridad del Reino Unido, dependiente del *Government Communications Headquarters*, una agencia de inteligencia del Reino Unido), de 28 de enero de 2020: https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector
- *5G PPP Phase1 Security Landscape* (grupo de trabajo sobre seguridad del grupo 5G PPP promovido por la Comisión europea), de junio de 2017: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

despliega la "Estrategia para el Impulso de la Tecnología 5G". Ambos documentos estratégicos han sido adoptados por el Consejo de Ministros, respectivamente, en julio y noviembre de 2020.

- Colectivos afectados:

  Como señala su artículo 4, la norma se aplicará a:

a) Las personas físicas o jurídicas que exploten redes 5G y a los prestadores de servicios de comunicaciones electrónicas basados total o parcialmente en dichas redes 5G.

   Esto incluye a operadores móviles titulares de concesiones administrativas para el uso del espectro radioeléctrico y a operadores móviles virtuales, así como a los operadores que utilicen la tecnología 5G para prestar servicios de comunicaciones. También incluye a los operadores que exploten redes privadas (o corporativas) de comunicaciones electrónicas, lo cual va a ser más frecuente con 5G de lo que es ahora con la tecnología 4G.

b) Los proveedores de equipos y servicios para la operación de las redes 5G, ajenos a los operadores (designados colectivamente en la norma como "suministradores").

   Los principales suministradores de componentes, programas y equipos para la gestión y control de las redes de comunicaciones móviles basadas en 5G en la actualidad son las empresas europeas Ericsson y Nokia y las chinas Huawei y ZTE.

   Una parte de la ley les afecta de manera directa, es decir, contiene disposiciones cuyo cumplimiento puede ser exigido, y sancionado, por las autoridades competentes. Se trata, por una parte, de las obligaciones de colaboración en las funciones de supervisión de la Administración, y, por otra, de los requisitos de certificación de productos, procesos o servicios, o de sometimiento a auditorías sobre el propio suministrador, que la ley autoriza a imponer.

   Pero además, la mayor parte de la ley les afecta de manera indirecta, pues los operadores de redes y servicios 5G son los principales destinatarios de ella, y los que les exigirán el cumplimiento de requisitos de seguridad. Este grupo de normas incluye disposiciones que pueden tener repercusiones importantes sobre los suministradores. Por ejemplo: la ley prevé que pueda exigirse a los operadores prescindir total o parcialmente de ciertos suministradores que se califiquen como de alto riesgo.

c) Los fabricantes o importadores de equipos terminales y dispositivos conectados.

   Nos referimos a los teléfonos fijos y móviles, a las tabletas, asistentes personales, y a la infinidad de objetos que podrán conectarse a las redes 5G, como automóviles, electrodomésticos, contadores, etc. Éstos conformarán la Internet de las cosas.

   Todos ellos pueden convertirse en vehículos de ataques tanto a la red como a los usuarios si no se tiene en cuenta la seguridad en su diseño y en su ciclo de vida.

.

d) Los usuarios corporativos de las redes 5G.

Pueden ser las entidades que gestionen una capa o segmento de la red para sus fines propios (por ejemplo: un hospital para sus aplicaciones de telemedicina). Debido a su imbricación con la red principal, pueden ser una puerta de entrada de un ataque exterior.

Además la norma, en cuanto asegura la seguridad de las redes y servicios 5G, beneficia a todos los usuarios de estas redes y servicios, así como a las Administraciones públicos que podrán comunicarse con ciudadanos y empresas de una forma más eficaz y segura.

- Interés público afectado:

El interés público afectado es el de garantizar la máxima protección de las redes y servicios de comunicaciones basadas en tecnología y redes 5G frente a ataques o incidentes de seguridad, como medio para cimentar la confianza en los nuevos servicios 5G.

Se desea fomentar el despliegue de los servicios 5G debido al potencial de esta tecnología para facilitar el desarrollo de aplicaciones innovadoras que favorezcan el crecimiento económico y social. Para ello, se ha de procurar un funcionamiento acorde a las expectativas generadas por las aplicaciones basadas en la tecnología 5G.

El estímulo de una demanda temprana por parte de los distintos sectores económicos de servicios basados en 5G va a depender, en parte, de la fiabilidad y robustez que ofrezcan las redes y servicios de comunicaciones electrónicas en los que se apoyarán todas esas nuevas aplicaciones. A la finalidad de garantizar la seguridad de esas redes y servicios responde esta ley.

- Por qué es el momento apropiado para hacerlo:

El despliegue masivo o a gran escala de las redes de comunicaciones móviles 5G tendrá lugar en segundo semestre de 2021.

Es oportuno que los operadores adapten sus políticas de ciberseguridad a las buenas prácticas recopiladas en el ámbito europeo antes de que los servicios estén disponibles. Así, las redes y servicios de comunicaciones móviles de quinta generación serán seguros desde el primer momento.

2. Objetivos.

La ley tiene por objetivo afianzar la confianza de consumidores y empresas en la fiabilidad de las redes y servicios 5G para el desarrollo de aplicaciones que exploten las posibilidades de la inteligencia artificial, la robótica, el Internet de las cosas y el "big data" en favor de distintos fines de interés económico y social, de modo que no existan recelos para su uso y quede garantizada la continuidad del servicio, su calidad y la confidencialidad de las comunicaciones y datos personales.

Como objetivo de fondo se encuentra el impulso al aprovechamiento de las comunicaciones móviles e inalámbricas basadas en 5G para el desarrollo de servicios de valor añadido para la sociedad en áreas tan diversas como los transportes, la sanidad, la industria manufacturera, la logística, la energía y los medios de comunicación. La tecnología 5G puede, además, ser muy útil para completar la transformación digital de la industria y los servicios.

Para ello, la ley aborda las amenazas provenientes de diversas fuentes, como la cadena de suministro para las redes, y establece obligaciones para tratar cada fuente de riesgo.

Así, uno de los sub-objetivos del anteproyecto es reforzar la seguridad de la cadena de suministro mediante el cumplimiento de requisitos técnicos que puedan ser exigidos a los proveedores, la diversificación de suministradores para evitar una excesiva dependencia de uno o varios de ellos, y las medidas que puedan adoptarse en cuanto a suministradores de alto riesgo.

Esta ley es un instrumento de la política pública de fomento de la tecnología 5G en Europa y en España. Otros elementos de esta política son la liberación de determinadas frecuencias radioeléctricas (actualmente ocupadas por la televisión digital terrestre) para su asignación a los servicios 5G[3] y la financiación de proyectos piloto para desarrollar entre operadores y agentes sectoriales servicios novedosos[4].

3. Alternativas.

Se han valorado las siguientes alternativas, antes de decidir elaborar la ley, para incrementar la seguridad de las redes y servicios 5G:

[3] Debe concluir antes de junio de 2020, según el Real Decreto 391/2019, de 21 de junio, por el que se aprueba el Plan Técnico Nacional de la Televisión Digital Terrestre y se regulan determinados aspectos para la liberación del segundo dividendo digital. Este plan trae causa de la Decisión (UE) 2017/899 del Parlamento europeo y del Consejo, de 17 de mayo de 2017, sobre el uso de la banda de frecuencia de 470-790 MHz en la Unión.

[4] La financiación pública de los proyectos piloto incluye fondos estatales y fondos FEDER (Fondo europeo de desarrollo regional).

- No dictar ninguna norma y seguir aplicando el artículo 44.1 de la Ley 9/2014, de 9 de mayo, general de telecomunicaciones. El aumento de actos maliciosos en la red y la elaboración de una recomendación específica de la Comisión Europea en la que se insta a los Estados miembros a colaborar en el establecimiento de unos estándares comunes de ciberseguridad 5G, aconsejan el dictado de una norma específica que establezca un marco común de seguridad para todos los operadores y prestadores de servicios.

- Animar a los operadores y prestadores de servicios a aplicar la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre ciberseguridad de las redes 5G: esta alternativa es una variación de la anterior, pues supone continuar con un enfoque autorregulatorio de la materia. Se considera que dada la importancia del 5G para la digitalización de la actividad productiva en multitud de ámbitos sectoriales, debe preverse un régimen de control y sanción en caso de incumplimiento. El refuerzo de las potestades de control públicas sobre la seguridad de las redes 5G es una de las medidas estratégicas destacadas en el citado toolbox.

- Aprobar, de acuerdo a lo establecido en el artículo 44.4 o en la disposición adicional décima de la Ley 9/2014, de 9 de mayo, un real decreto o una orden ministerial de instrucciones que recojan las obligaciones y medidas necesarias para reforzar la seguridad de las redes y servicios 5G.

Tal y como se señala en el propio toolbox, la importancia de la seguridad de las redes 5G exige adoptar normas de obligado cumplimiento y sanciones que garanticen la correcta seguridad de esta tecnología en Europa. Por tanto, se ha considerado que la fijación de determinadas obligaciones que como la diversificación de suministradores, pueden llegar a afectar a la libertad de empresa, y de las correspondientes sanciones, encuentra mejor acomodo en una norma con rango de Ley.

Sin embargo, la presente Ley en aras de facilitar la rápida modificación y la flexibilidad de una norma dirigida a abordar riesgos cambiantes en un entorno basado en la innovación se limita a establecer criterios y obligaciones generales, remitiendo su concreción al Esquema de seguridad para las redes y servicios 5G, que se aprobará mediante norma reglamentaria o a otras normas de carácter reglamentario que puedan aprobarse, de conformidad con la disposición final segunda.

4. Adecuación a los principios de buena regulación.

La ley cumple con los principios de buena regulación enunciados en el artículo 129 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas.

En cuanto a los principios de necesidad y eficacia, el anteproyecto se justifica por dos razones de interés general, que son asegurar la máxima protección a los usuarios de la tecnología 5G para fines personales o profesionales y fomentar el crecimiento económico por medio de la digitalización y la innovación.

Los fines de la ley están relacionados con los intereses públicos que se protegen. En el artículo 2 se expresa el fin inmediato de aquella, que es garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, y la seguridad nacional. Este fin es importante por sí solo, ya que hay derechos fundamentales implicados, como el derecho a la intimidad personal y familiar y al secreto de las comunicaciones, e intereses comerciales en juego; pero, también actúa como apoyo para promover la adopción temprana del 5G y el aprovechamiento de todas sus posibilidades para el desarrollo económico, que es el fin último de la ley.

Como ya se ha visto al analizar la elección de una norma con rango de Ley se considera que este instrumento es el más eficaz para lograr este fin.

El principio de proporcionalidad se predica de la sustancia de la norma. El anteproyecto impone dos obligaciones especiales en relación con la tecnología 5G a los operadores: realizar un análisis de riesgos y adoptar las medidas adecuadas para evitarlos. Algunas de estas medidas, como las relativas a la política de permisos de acceso no suponen gran variación respecto a las medidas de seguridad que están en vigor hace tiempo en el sector. Sin embargo, otras medidas, en particular, las relativas a la diversificación de suministradores ya que si el operador tiene un solo proveedor o varios con un alto perfil de riesgo, sí son novedosas y su cumplimiento de la norma puede llegar a implicar la rescisión de contratos en vigor, por lo que siempre que el Esquema de seguridad para redes y servicios 5G imponga este tipo de medidas será necesario justificarlo y ponderar su coste para los operadores y las consecuencias que puede tener para el despliegue de las redes y el acceso de los usuarios al servicio. Se podrán prever, además, períodos transitorios para ejecutar el cambio de proveedores.

Además, debe tenerse en cuenta que tanto las medidas atinentes a la protección del núcleo de red como a la cadena de suministro están tomadas de la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre la ciberseguridad de las redes 5G y del "toolbox", por lo que se trata de medidas que serán también adoptadas en todo el ámbito europeo.

Por lo que respecta al principio de seguridad jurídica, el anteproyecto se encuadra en la Ley 9/2014, de 9 de mayo, y pertenece al bloque normativo propio del sector de las telecomunicaciones. Ambas cosas se explicitan en la ley.

La Ley traslada a norma las medidas contenidas en la caja de herramientas resultado del desarrollo de la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre Ciberseguridad de las redes 5G.

De acuerdo con lo establecido en el artículo 10.4 del anteproyecto, la normativa comunitaria también deberá tenerse en cuenta a la hora, de elaborar el Esquema de Seguridad de las redes y servicios 5G, garantizándose, de esta manera, la coherencia entre la ley y el Ordenamiento jurídico comunitario.

Por su parte la propia Ley, como ya se ha dicho remite a una norma reglamentaria concreta: el Esquema de seguridad de las redes y servicios 5G la concreción de sus extremos, previéndose en su disposición final segunda la habilitación al Gobierno para el desarrollo reglamentario de lo dispuesto en la Ley.

Las obligaciones de publicidad activa relativa a los documentos que integran el expediente de elaboración de esta ley y las de participación de los ciudadanos y empresas en su elaboración se cumplirán durante la tramitación de la norma. Por lo demás, se cumple el deber de definir con claridad los objetivos que persigue la norma y su justificación en la Exposición de Motivos. Con esto se da por satisfecho el principio de transparencia en los términos establecidos en el artículo 129.5 de la Ley 39/2015, de 1 de octubre.

El principio de eficiencia demanda la reducción de cargas administrativas. Éstas pueden ser, por ejemplo, una solicitud, una obligación de comunicar datos, de conservar documentos o de formalizarlos; en definitiva, es toda actividad de naturaleza administrativa que debe llevar a cabo una empresa o un ciudadano para cumplir con las obligaciones derivadas de la normativa[5]. En el apartado sobre cargas administrativas se valoran las que la norma establece, que en todo caso han sido las mínimas necesarias para cumplir el objetivo perseguido por la Ley.

Por lo demás, el anteproyecto no incide de forma relevante en los recursos públicos. Las funciones requeridas para su aplicación –las de tratamiento de la información recibida de los operadores, análisis de riesgos nacional y control del cumplimiento de sus disposiciones- pueden ser asumidas por los órganos que ya desempeñan funciones de supervisión de la seguridad de las redes y servicios de comunicaciones electrónicas en el Ministerio de Asuntos Económicos y Transformación Digital.

B. CONTENIDO Y ANÁLISIS JURÍDICO

1. Contenido.

[5] http://www.mptfp.es/portal/funcionpublica/gobernanza-publica/simplificacion/que-es-carga.html

El anteproyecto consta de una Exposición de Motivos, 22 artículos divididos en cuatro capítulos, dos disposiciones adicionales, una disposición transitoria y tres disposiciones finales.

Capítulo I. Disposiciones generales:

El primer capítulo se titula "Disposiciones generales" y contiene cinco artículos.

El artículo primero define su objeto; el segundo, sus fines, el tercero se dedica a definiciones; el cuarto delimita su ámbito de aplicación y el quinto establece la aplicación supletoria de la normativa sobre seguridad e integridad de las redes de comunicaciones electrónicas.

La definición de "redes 5G" está inspirada en la definición de "redes 5G" que ofrece la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, sobre la ciberseguridad de las redes 5G.

El ámbito de aplicación de la ley abarca a todos los actores de la cadena de valor de las redes y servicios 5G, pues se parte de la premisa de que la seguridad de 5G incumbe a todos los agentes de ésta. En primer lugar estarían los operadores de redes y los prestadores de servicios de comunicaciones electrónicas que utilicen la tecnología 5G. En segundo lugar, los suministradores o proveedores de equipos y servicios para la explotación de redes 5G. En tercer lugar, se encuentran los fabricantes de equipos terminales y dispositivos conectados a las redes 5G y por último estarían los usuarios corporativos.

El artículo 5 integra esta norma dentro del conjunto de leyes y reglamentos que regulan la seguridad de las redes de información, constituido, fundamentalmente, por la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, y su normativa de desarrollo, que serán de aplicación supletoria.

Capítulo II. Análisis y gestión de los riesgos:

El capítulo II se titula "Análisis y gestión de los riesgos" y comprende los artículos 6 a 9.

Los análisis de riesgo son el primer elemento de toda política de gestión de la seguridad. El segundo es la adopción de medidas que sean apropiadas para abordar los riesgos que, en cada caso, se hayan identificado. Por tanto, aunque los riesgos pueden ser similares y existe un abanico común de medidas de seguridad, su aplicación debe particularizarse para cada operador.

En este capítulo, se regulan los análisis de riesgos que deben efectuar los operadores, al menos, cada dos años. Siguiendo fielmente el análisis coordinado de riesgos en la UE y el "toolbox", los operadores deberán poner especial atención en el análisis de los riesgos que afecten a los componentes y funciones esenciales de las redes 5G, que se enumeran en el artículo 6.2. El artículo 6.3 cita los factores, que, como mínimo, habrán de tenerse en cuenta al

realizar los análisis, que incluyen, entre otros, la dependencia de determinados suministradores o proveedores en elementos o funciones esenciales de la red, las estrategias de permiso de acceso a activos físicos y lógicos , los agentes externos, incluyendo grupos organizados con capacidad para atacar la red o la interrelación con otros servicios esenciales para la sociedad (lo que se ha llamado "dependencia circular").

Dada la relevancia de los suministradores en la explotación de las funciones características de la tecnología 5G, en el artículo 7 se obliga a los operadores a analizar las prácticas de seguridad de sus suministradores.

En el artículo 8 se regula el deber de los operadores de gestionar sus riesgos y los de sus suministradores a los que deberán exigir el cumplimiento de estándares de seguridad, desde el diseño de los productos hasta su puesta en funcionamiento, así como el control de su propia cadena de suministro. Al gestionar sus riesgos tendrán en cuenta el análisis de riesgos nacional y el Esquema de seguridad para las redes y servicios 5G, a los que se refiere el Capítulo siguiente.

Además, los operadores deberán elaborar una estrategia de diversificación de suministradores con medidas para limitar la dependencia de partes o funciones esenciales de la red de un solo suministrador o de varios que tengan una calificación de riesgo alto, incluyendo plazos para restringir o excluir la presencia de suministradores de alto riesgo en dichos elementos y funciones.

De acuerdo con el artículo 9, los operadores deberán remitir al Ministerio de Asuntos Económicos y Transformación Digital los resultados de los análisis de riesgo que realicen, una descripción de las medidas técnicas y organizativas para mitigarlas, y un informe sobre las prácticas de seguridad de sus suministradores y sus modificaciones, así como remitir al citado Ministerio su estrategia de diversificación de suministradores e informarle cada año sobre su estado de ejecución.

Los análisis de riesgos elaborados por los operadores nutrirán el análisis de riesgos a nivel nacional y el Esquema de seguridad para las redes y servicios 5G para hacer frente a dichos riesgos a la que se refiere el capítulo siguiente.

Capítulo III. Esquema de seguridad de las redes y servicios 5G

El Capítulo III se titula Esquema de seguridad de las redes y servicios 5G y comprende los artículos 10 a 18.

De acuerdo con el artículo 10, el análisis de riesgos a nivel nacional constituirá la base del Esquema de seguridad de las redes y servicios 5G, que será aprobado por el Gobierno, mediante real decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital para garantizar la robustez del sistema de comunicaciones basadas en 5G a nivel nacional. El Gobierno cooperará estrechamente con otros Estados miembros y con la Comisión europea

en todo lo relativo al Esquema de seguridad de las redes y servicios 5G, a la definición del perfil de riesgo de los suministradores y a la aplicación de las medidas de apoyo que la Comisión europea impulse. El Esquema de seguridad para las redes y servicios 5G será informado por el Consejo de Seguridad Nacional, y se revisará al menos cada seis años o cuando las circunstancias lo requieran

El artículo 11 ofrece los criterios que tendrá en cuenta el Gobierno al examinar el perfil de riesgo de los suministradores de los operadores de redes y servicios 5G en España. Estos criterios, que son los que figuran en el "toolbox" europeo se refieren, tanto a las garantías técnicas de funcionamiento y protección frente a ataques como a su exposición a injerencias externas. Entre ellos se encuentran el sometimiento a auditorías externas, el cumplimiento de normas o especificaciones técnicas, la composición de su capital social y la estructura de sus órganos de gobierno, los vínculos de los suministradores y de su cadena de suministro, con los gobiernos de terceros países, o las características del régimen político y de la política de ciberdefensa, de ese tercer Estado.

El Gobierno, mediante Acuerdo de Consejo de Ministros, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital y previo informe del Consejo de Seguridad Nacional, calificará como bajo, medio o alto el perfil de riesgo de los suministradores según los resultados del análisis de las vulnerabilidades y especificará las consecuencias de dicha calificación

El artículo 12 señala que el Esquema de seguridad para las redes y servicios 5G contendrá una priorización de los riesgos, que tendrá en cuenta las aportaciones al alcance de cada agente de la cadena de valor de 5G para garantizar un funcionamiento continuado y seguro de la red y los servicios, fijando las obligaciones que aplican a operadores, suministradores y a equipos terminales y dispositivos conectados, así como los requisitos para la contratación pública de comunicaciones 5G o de servicios que se basen en estas redes.

El artículo 13 señala que el Esquema de seguridad para las redes y servicios 5G permite establecer plazos máximos y medidas de apoyo de implementación de las obligaciones que se fijen, que se entenderán sin perjuicio de la aplicación de los instrumentos de control sobre inversiones extranjeras directas en los operadores de redes y servicios 5G o en los suministradores españoles, y de la denuncia de conductas contrarias a la competencia en el mercado de suministros ante la Comisión europea o la Comisión Nacional de los Mercados y la Competencia, según proceda.

El artículo 14 contiene dos listados no cerrados de las obligaciones que el Esquema de Seguridad para las redes y servicios 5G puede llegar a imponer a operadores y suministradores, entre las que se encuentran para los primeros la de adoptar determinados criterios para seleccionar e identificar a las personas que puedan acceder a los activos físicos y lógicos de la red y para el mantenimiento de registros de acceso o la prohibición de utilizar equipos, programas o servicios de suministradores de una determinada calificación de riesgo, incluyendo

el establecimiento de cuotas o porcentajes de utilización, así como plazos para su eliminación de las redes. Asimismo, a operadores o suministradores, según proceda, se les podrán imponer, entre otras posibles obligaciones, el cumplimiento de normas o especificaciones técnicas aplicables a redes y sistemas de información o el sometimiento de los equipos y programas utilizados para la operación de las redes 5G a una auditoría o control externo por una entidad u organismo acreditado.

Asimismo, el esquema de seguridad para las redes y servicios 5G podrá fijar objetivos de diversificación de suministradores en la cadena de suministro de los operadores y para el conjunto del Estado, en función del cual podrán imponerse obligaciones de sustitución o ampliación del número de suministradores para toda la red, para componentes importantes de éstas, para determinados clientes, o en determinadas partes del territorio. Se podrán prever, también plazos transitorios para el cumplimiento de las obligaciones para los operadores, suministradores, fabricantes o quienes pongan en el mercado equipos terminales y dispositivos conectados y para los usuarios corporativos.

El artículo 15 se refiere a la certificación en elementos de redes 5G y requisitos esenciales para equipos terminales y dispositivos conectados, conforme a la normativa comunitaria

El artículo 16 permite aplicar las obligaciones de manera diferenciada a los distintos sujetos obligados y en distintos plazos o fases en supuestos debidamente justificados.

El artículo 17 sobre apoyo a la I+D+i en Ciberseguridad 5G señala que en el Esquema de seguridad para las redes y servicios 5G incluirá las líneas generales y prioridades de las ayudas públicas y fomentará la interoperabilidad de los equipos y programas ligados a la gestión de redes 5G, así como la participación de actores públicos y privados en la elaboración de estándares internacionales sobre el funcionamiento de las redes y servicios 5G.

El artículo 18, referido a las redes y servicios 5G en la contratación pública, señala que cuando la Administración licite un contrato de comunicaciones o de servicios que hagan uso de la tecnología 5G, se exigirá para su adjudicación, cuando sea procedente, la posesión de una certificación derivada de un esquema de certificación europeo aprobado conforme al Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad, que sea pertinente según el objeto del contrato. De modo motivado, podrá imponerse la condición de excluir el uso de suministradores que tengan una determinada calificación de riesgo de un contrato público.

Capítulo IV. Potestades administrativas de control y sanción:

El capítulo IV regula la inspección y el control de la aplicación de la ley y de la Estrategia de seguridad, y consta de 4 artículos, del 19 al 22

El artículo 19 establece que el Ministerio de Asuntos Económicos y Transformación Digital será competente para aplicar el Esquema de seguridad para las redes y servicios 5G a los operadores, suministradores y fabricantes de equipos terminales y dispositivos conectados o a quienes los pongan en el mercado. En todo lo que afecte a los suministradores de alto riesgo, actuará bajo la coordinación del Consejo de Seguridad Nacional.

Los demás departamentos ministeriales aplicarán las obligaciones de seguridad referidas a los usuarios corporativos que contenga el Esquema de seguridad para las redes y servicios 5G. Por ejemplo, el Ministerio de Sanidad lo hará sobre los hospitales que utilicen aplicaciones de telemedicina.

Se incorpora, asimismo, en este artículo una referencia a la coordinación del Ministerio de Asuntos Económicos y Transformación Digital en la aplicación de los criterios que pueden condicionar la aplicación de las medidas de seguridad (los que el "toolbox" denomina "implementing factors") para que las decisiones que se adopten sean eficaces, pero proporcionadas. Se deberán tener en cuenta, a este respecto, la prioridad que tenga conjurar el riesgo detectado, el coste para los operadores y las repercusiones para los planes de despliegue de redes y el acceso de los usuarios a los servicios.

Por último, se enumeran las potestades administrativas que pueden ejercer los órganos competentes para la aplicación de la ley, entre las que se incluye la adopción de instrucciones técnicas y resoluciones para concretar las obligaciones que incumben a cada sujeto o grupo de sujetos

El artículo 20 establece un trámite de audiencia obligatorio antes de dictar instrucciones técnicas, guías orientativas y resoluciones, y alienta la participación del público en general en la elaboración de las instrucciones técnicas.

En el artículo 21 atribuye al Ministerio de Asuntos Económicos y Transformación Digital, en la aplicación y supervisión de lo establecido en esta ley, todas las potestades de la función inspectora previstas en el Título VIII de la Ley 9/2014, de 9 de mayo. Asimismo se refiere este artículo a las obligaciones de información de los sujetos obligados.

El artículo 22 relativo al régimen sancionador establece que será de aplicación el régimen sancionador establecido en el Título VIII de la Ley 9/2014, de 9 de mayo.

Adicionalmente, se tipifican 2 nuevas infracciones graves (el incumplimiento de las obligaciones establecidas en el Esquema de seguridad para las redes y servicios 5G cuando sean directamente exigibles y el incumplimiento de las resoluciones dictadas por órganos competentes) y 1 leve (el incumplimiento de los requerimientos de información y de colaboración dictados por los órganos competentes), que se transformará en infracción grave cuando el requerimiento se dirija a los operadores o a los suministradores y haya pasado un mes desde la finalización del plazo para su cumplimiento.

Las sanciones por la comisión de infracciones muy graves, llevan aparejada multa de hasta 20.000.000 euros. También podrán comportar la prohibición para contratar prevista en el art. 71 de la Ley 9/2017 de Contratos del Sector Público. Por la comisión de infracciones graves, la sanción será de multa de hasta 2.000.000 euros y por la comisión de infracciones leves la sanción será de amonestación o multa hasta 50.000 euros.

En el caso de que se acredite fehacientemente que el perjuicio causado o el beneficio obtenido con las prácticas sancionadas, supera estas cuantías, la sanción se incrementará hasta dicho importe.

Los órganos competentes para la aplicación del Esquema de seguridad para las redes y servicios 5G lo son también para la aplicación del régimen sancionador a los sujetos a los que, respectivamente, supervisen.

Parte final:

En la disposición adicional primera se fija un plazo de 4 meses para que los operadores de redes que ya estuvieran prestando servicios 5G o los que tengan previsto hacerlo en los próximos dos años, remitan al Ministerio de Asuntos Económicos y Transformación Digital sus análisis de riesgos y un informe sobre sus suministradores, los productos o servicios contratados con ellos y un análisis de sus prácticas de seguridad. Los operadores de redes deberán remitir actualizaciones periódicas de estos informes en el plazo de 4 meses desde su realización.

La disposición adicional segunda establece que la Ley aplicará a las sucesivas generaciones comunicaciones electrónicas mientras no exista normativa específica.

La disposición transitoria señala que hasta la aprobación del Esquema de seguridad para las redes y servicios 5G, se habilita al titular del Ministerio de Asuntos Económicos y Transformación Digital, previo informe del Consejo de Seguridad Nacional, a establecer las obligaciones relacionadas con el perfil de riesgo de los suministradores que se consideran en el artículo 14.

La disposición final primera señala como competencias al amparo de las que se dicta la ley las establecidas a favor del Estado en materia de telecomunicaciones y de seguridad pública en los artículos 149.1.21ª y 149.1.29ª de la Constitución.

En la disposición final segunda se habilita al Gobierno para desarrollar reglamentariamente lo previsto en esta ley.

En la disposición final tercera se fija como fecha de entrada en vigor el día siguiente al de la publicación oficial de la ley.

Conforme a lo dispuesto en el segundo párrafo del artículo 23 de la Ley 50/1997, de 27 de noviembre, del Gobierno- “Disposiciones de entrada en vigor”- se justifica la entrada en vigor

el día siguiente al de su publicación en el "Boletín Oficial del Estado", por la necesidad urgente de garantizar la seguridad de las redes 5G antes de su despliegue masivo.

2. Análisis jurídico.

- Relación con otras normas nacionales.

  - La Ley 9/2014, de 9 de mayo (especialmente su artículo 44), recoge obligaciones de seguridad genéricas que los operadores de redes 5G siguen teniendo que cumplir. Además por remisión del Anteproyecto aplica asimismo su régimen sancionador.

  - El Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, establece requisitos que deberán seguir cumpliendo los operadores que hayan sido designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

  - La Orden IET/1090/2014, de 16 de junio, por la que se regulan las condiciones relativas a la calidad de servicio en la prestación de los servicios de comunicaciones electrónicas regula, en su capítulo VI, la obligatoria notificación a las Autoridades de los casos de interrupción del servicio telefónico y de acceso a Internet y su y el capítulo VII, la potestad inspectora de la Secretaría de Estado para el Avance Digital en esta materia.

- Coherencia con el Derecho de la Unión Europea:

  - El Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y la Directiva 2002/58/CE del Parlamento europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), transpuesta al ordenamiento jurídico español a través del capítulo III del título III y los artículos 48 y 49 de la Ley 9/2014, de 9 de mayo, también se relacionan con esta norma, ya que el refuerzo de la seguridad en las redes 5G redundará en una mayor protección frente a intromisiones ilegítimas en los derechos a la intimidad y al secreto de las comunicaciones en este ámbito.

- El presente anteproyecto trae causa directa del desarrollo de la Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G, en la que se propone una acción coordinada de los Estados miembros para analizar los riesgos de seguridad de la tecnología 5G y la recopilación y aplicación de buenas prácticas que garanticen la seguridad de estas redes. Los Estados miembros apoyaron esta Recomendación en las conclusiones acordadas por el Consejo de la Unión Europea de 3 de diciembre de 2019. En concreto, tuvo como resultado el desarrollo de una "caja de herramientas" que se comenta más adelante.

- El Reglamento UE 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre la ciberseguridad, regula el procedimiento conforme al que podrán adaptarse los esquemas europeos de certificación de la ciberseguridad de las tecnologías de la información y la comunicación, a los que aluden los artículos 15.1 y 18 de la ley.

- El día 29 de enero de 2020, se publicó la "caja de herramientas" o "toolbox" europeo[6]. Ese mismo día, la Comisión europea emitió la Comunicación "Despliegue seguro de la 5G en la UE - Aplicación de la caja de herramientas de la UE" en la que se señala que las conclusiones y acciones recomendadas en el l "toolbox" han de ser "medidas clave" que deben implementar los Estados miembros y la Comisión europea para garantizar la seguridad de estas redes en Europa. La Comunicación fija un calendario para recopilar información sobre el estado de ejecución del "toolbox" antes del final de 2020, y enumera los instrumentos comunitarios que la Comisión empleará para desarrollar las acciones que le competen.

- Normas que se modifican o derogan y futuras normas:

  El anteproyecto de ley no modifica ni deroga ninguna norma.

De acuerdo con lo establecido en el artículo 10.1 del Anteproyecto, el Gobierno aprobará, mediante real decreto, a propuesta del Ministerio de Asuntos Económicos y Transformación Digital, un Esquema de seguridad para las redes y servicios 5G para abordar los riesgos que pongan de manifiesto los análisis que se efectuarán a nivel nacional. Este esquema será el que concrete todas las medidas previstas en el Anteproyecto.

[6] *Cybersecurity of 5G networks. EU toolbox of risk mitigating measures*, publicado el 29 de enero de 2020. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

C. ADECUACIÓN AL ORDEN DE DISTRIBUCIÓN DE COMPETENCIAS

El anteproyecto de ley no afecta a las competencias de las Comunidades Autónomas al dictarse en virtud de las competencias exclusivas en materia de telecomunicaciones y seguridad pública atribuidas al Estado por los artículos 149.1.21ª y 149.1.29ª de la Constitución.

D. IMPACTO ECONÓMICO Y PRESUPUESTARIO.

1. Impacto económico general.

El sector de las comunicaciones electrónicas se caracteriza por un elevado grado de dinamismo e innovación, que por lo general ha estado ligado a la inversión en el despliegue de nuevas redes.

En la actualidad existe la oportunidad de continuar con esta dinámica innovadora, mediante la inversión redes 5G, pero ello solo será posible si se introducen las medidas adecuadas que garanticen la integridad, continuidad y seguridad de estas redes, evitando los riesgos que su implantación generalizada podría llegar a provocar.

Por ello, la Ley introduce la posibilidad de que el Esquema de seguridad de las redes y servicios 5G establezca aquellas medidas recomendadas en la normativa comunitaria que mejor se adapten a los riesgos identificados en los análisis de riesgos efectuados a nivel comunitario y nacional.

Pero es que además, las telecomunicaciones, por su carácter transversal, no solo garantizan la prestación de servicios cada día más necesarios como el teletrabajo, la telemedicina o la enseñanza online, sino que al tiempo favorecen el crecimiento de otros sectores como la industria de los contenidos, el Big Data, el Internet de las Cosas o la automoción conectada, permitiendo, asimismo, la gestión inteligente del transporte y de los recursos energéticos y la reducción de la brecha digital entre los distintos territorios.

En este sentido, las nuevas redes 5G, se sitúan como una pieza clave para acelerar la transformación digital de la sociedad y la economía.

En nuestro entorno más inmediato, los análisis de la Comisión Europea prevén que los beneficios estimados al introducir 5G en cuatro sectores productivos (automoción, salud, transporte y utilities) aumentarían progresivamente hasta alcanzar en 2025 los 62.500 millones de euros de impacto directo anual dentro de la Unión Europea, que se elevarían a 113.000 millones de euros sumando los impactos indirectos. El mismo estudio estima que en nuestro

país se obtendrían unos beneficios indirectos en los cuatro sectores analizados de 14.600 millones de euros y una importante creación de empleos.

En conclusión, debe señalarse que en el actual momento de incertidumbre internacional, las telecomunicaciones constituyen uno de los sectores más dinámicos de la economía y uno de los que más pueden contribuir, por su carácter transversal, al crecimiento, la productividad y al empleo, y por tanto, al desarrollo económico y al bienestar social

Asimismo se prevé que las medidas de seguridad propuestas en el Anteproyecto tengan un impacto neutro en los precios, ya que los operadores y prestadores de servicios ya están realizando fuertes inversiones para ofrecer conectividad a través de 5G, siendo la seguridad es un aspecto marginal de esos costes.

Las medidas más costosas pueden ser las de certificación de equipos o de auditoría empresarial, para el operador o el suministrador sobre el que recaiga la obligación, y las de sustitución de suministradores o incremento del número de suministradores que trabajan con el operador. Por eso, antes de decidir la adopción de una de estas medidas, las autoridades públicas deberán hacer un análisis de costes y ponderar sus efectos negativos, estableciéndose de conformidad con lo previsto en el "toolbox" que su ejecución podrá ser gradual.

En todo caso, el esfuerzo económico dedicado a medidas de seguridad debe considerarse como una inversión, puesto que reduce los gastos en reposición del servicio y en posibles indemnizaciones, aumentando asimismo los ingresos por la entrada de nuevos clientes que confían en la nueva tecnología.

Como ya se dijo, por su impacto transversal la introducción de la tecnología 5G está llamada a crear un importante efecto positivo en el empleo de numerosos sectores.

Pero además el cumplimiento de las concretas medidas de seguridad previstas en esta ley puede tendrá también un efecto positivo para la creación de empleo en sectores como la I+D+I, la certificación o la auditoria, señalándose en el artículo 2 del Anteproyecto como objetivo el de fortalecer la industria y fomentar la I+D+i nacionales en Ciberseguridad y en su artículo 17.2 que el Esquema de seguridad para las redes y servicios 5G incluirá las líneas generales y prioridades de las ayudas públicas que pudieran ser convocadas para fomentar la investigación y el desarrollo en materia de seguridad en las redes 5G y en los servicios que dependan de ellas, y para la formación de personal especializado.

El efecto de la ley sobre los consumidores se prevé también positivo, ya que a la mayor posibilidad de elección entre tecnologías que deriva de la propia introducción del 5G, se suman los beneficios intangibles asociados a una mayor seguridad y confianza en el uso de la nueva tecnología.

2. Efectos en la competencia y en la unidad de mercado.

La norma tiene determinados efectos positivos en cuanto promueve la interoperabilidad de los equipos y programas.

Además, las disposiciones relacionadas con la diversificación de proveedores en la cadena de suministro y las medidas destinadas a fortalecer la industria y fomentar la I+D+I nacionales en Ciberseguridad (artículo 17) pueden contribuir a la aparición y crecimiento de nuevos actores.

Por otro lado, aunque la norma establece determinadas limitaciones a la libre competencia (como la posibilidad de restringir la participación de los suministradores de alto riesgo) estas restricciones no solo favorecen la confianza de los usuarios sino que al tiempo salvaguardan la seguridad nacional, dada la importancia de muchos de los servicios y aplicaciones que descansaran sobre estas redes (salud, protección civil, educación…)

En este sentido, de acuerdo con lo establecido en la Recomendación y en el toolbox, las medidas a las que se refiera el Esquema de seguridad para las redes y servicios 5G, serán únicamente aquellas imprescindibles, a la vista de un riguroso análisis de riesgo y de las decisiones tomadas por otros Estados miembros o por la propia UE, concediéndose plazos transitorios para su aplicación, de modo que se minimicen las repercusiones sociales y económicas para operadores y usuarios.

3. Impacto presupuestario

- Desde el punto de vista de los ingresos:

El anteproyecto no implicará la generación o precepción de ingresos para la Hacienda estatal ni para la Hacienda de otras Administraciones Públicas.

- Desde el punto de vista del gasto:

Las funciones de supervisión y control incluidas en este anteproyecto de ley serán atendidas con las disponibilidades presupuestarias existentes en cada ejercicio y con los medios personales existentes y no supondrán incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

E. DETECCIÓN Y MEDICIÓN DE CARGAS ADMINISTRATIVAS.

A continuación se analizan las cargas administrativas que los artículos 6 a 9 del Anteproyecto imponen a operadores de redes y servicios de comunicaciones electrónicas.

Por su parte, los artículos 14 y 15 del Anteproyecto prevén que, posteriormente, el Esquema de seguridad de las redes y servicios 5G o el Gobierno puedan imponer obligaciones

diferenciadas a operadores o suministradores concretos o a los fabricantes o comercializadores de determinados equipos terminales o dispositivos conectados. Se considera que el análisis de dichas cargas habrá de realizarse cuando las mismas efectivamente se impongan

- **Realizar al menos cada 2 años un análisis de riesgos de las redes y servicios 5G (artículo 6) y remitirlo al Ministerio de Asuntos Económicos y Transformación Digital (artículo 9)**

El artículo 6 del Anteproyecto obliga a los operadores a efectuar al menos cada dos años un análisis de los riesgos de las redes y servicios 5G, considerando tanto los que afecten a elementos y funciones esenciales de las redes 5G como otros riesgos propios de las redes de comunicaciones electrónicas.

Por su parte el artículo 9 obliga a remitir estos análisis a la Administración

Al respecto, cabe señalar que el análisis y gestión de los riesgos de ciberseguridad es una actividad que realizan de modo habitual ya los operadores, y para los que el anteproyecto tan sólo establece unas mínimas pautas de actuación para adecuarse a las particularidades del entorno 5G.

El artículo 44.4 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, ya da por supuesto que los operadores documentan sus políticas de seguridad. Lo mismo hacen los artículos 32.1 y 33.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

En este sentido, se considera que la realización de estos análisis, además de ser una obligación totalmente imprescindible para garantizar la seguridad de los servicios públicos esenciales que en el futuro puedan prestarse a través de estas redes, supone una práctica común para los operadores, ya que protege sus propios planes de negocio y el mantenimiento y ampliación de su cartera de clientes.

- **Describir las medidas técnicas y organizativas adoptadas para mitigar los riesgos (artículo 8), analizar, al menos cada dos años, las prácticas de seguridad de los suministradores (artículo 7 y 8), y remitirlo todo al Ministerio de Asuntos Económicos y Transformación Digital (artículo 9)**

De acuerdo con el artículo 7 del anteproyecto, los operadores deberán examinar las prácticas de seguridad de sus suministradores que puedan repercutir en los productos y servicios que les proporcionan, teniendo en cuenta los factores de riesgo. Este examen debe repetirse, al menos, cada dos años.

Por su parte el artículo 9 obliga a los operadores a remitir al Ministerio una descripción de las medidas técnicas y organizativas adoptadas para mitigar los posibles riesgos, y un informe sobre las prácticas de seguridad de sus suministradores así como sus modificaciones.

Tal y como se dijo en el apartado anterior se considera que el análisis de las medidas de seguridad de sus proveedores es ya una práctica habitual entre los operadores que no pueden arriesgarse a que los fallos de seguridad de un suministrador ponga en riesgo sus planes de negocio, estando generalizada la inclusión de cláusulas relativas a requisitos de seguridad en los contratos entre operadores y suministradores por lo que no se prevé tampoco especialmente costosa la imposición a los operadores de la obligación de exigir a sus proveedores el cumplimiento de estándares de seguridad, desde el diseño de los productos hasta su puesta en funcionamiento, así como el control de su propia cadena de suministro

- **Elaborar una estrategia de diversificación de suministradores (artículo 8.3) e informar cada año al Ministerio de Asuntos Económicos y Transformación Digital sobre su estado de ejecución (artículo 9.2)**

El artículo 8.2 obliga a los operadores a elaborar una estrategia de diversificación de suministradores con medidas para limitar la dependencia de partes o funciones esenciales de la red de un solo suministrador o de varios que tengan una calificación de riesgo alto, incluyendo plazos para restringir o excluir la presencia de suministradores de alto riesgo en dichos elementos y funciones.

Por su parte, el artículo 9.2 obliga a los operadores a remitir su estrategia de diversificación de suministradores al Ministerio y a informarle cada año sobre su estado de ejecución.

No puede determinarse la magnitud de la carga administrativa que implicará estas cargas al no saber cuántos prestadores de los inscritos en el Registro de operadores previsto en el artículo 7 de la Ley 9/2014, de 9 de mayo, optarán por ofrecer servicios en 5G en el futuro.

En todo caso, la utilización de medios telemáticos para la remisión de la documentación a la Administración mitiga la carga que esta obligación de información pueda suponer para el operador. Asimismo, de acuerdo con lo establecido en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones que es de aplicación supletoria Se respetará siempre el deber de confidencialidad respecto a la información comercial sensible que puedan remitir los operadores

Por último, en relación con el posible impacto de las cargas en Pequeñas y Medianas Empresas (PYMES) debe señalarse que la mayor parte de los operadores que explotan redes y prestan servicios de comunicaciones electrónicas no tienen dicho tamaño, por lo que no se verán afectadas por dichas cargas, mientras que, sin embargo, miles de PYMES que ofrecen servicios en las redes sí se beneficiaran del ecosistema 5G seguro que persigue la norma.

F. IMPACTO POR RAZÓN DE GÉNERO

El Anteproyecto tiene un impacto de género nulo, en la medida en que su contenido no incluye ningún tipo de medida que pueda atentar contra la igualdad de oportunidades entre hombres y mujeres.

G. IMPACTO EN LA LUCHA CONTRA LA DESPOBLACIÓN Y EL CAMBIO CLIMÁTICO

La seguridad de la tecnología 5G se configura como una pieza clave para la vertebración territorial del país, ya que el acceso seguro a las nuevas redes y a los nuevos contenidos y servicios digitales que podrán prestarse a través de las mismas, son un elemento imprescindible para la incorporación de la ciudadanía y de las empresas a la Sociedad de la Información y del Conocimiento, fomentando con ello la cohesión social y el desarrollo económico y contribuyendo al desarrollo de la nueva Administración Electrónica.

En este sentido las medidas que introduce la Ley se convierten en importantes pilares para conseguir la eliminación de la brecha digital y la vertebración de los distintos territorios, de modo que el acceso a nuevos servicios y aplicaciones como los de telemedicina, aprendizaje online o teletrabajo quede garantizado en cualquier parte del territorio español, favoreciendo el asentamiento y la fijación de población en el medio rural.

A ello se une la importancia de las telecomunicaciones como factor clave para la lucha contra el cambio climático. En este contexto, se enmarca el objetivo establecido por la Unión Europea de reducir en un 40% las emisiones de gases de efecto invernadero para el año 2030, con relación a los niveles de 1990.

El sector de las Tecnologías de la Información y Comunicación es un sector que genera un bajo nivel de emisiones relativo, y a la vez su papel puede ser fundamental en la lucha frente al cambio climático al facilitar un uso más eficiente de los recursos energéticos por otros sectores.

En este sentido deben resaltarse los ahorros energéticos de las propias redes, gracias a la mayor eficiencia energética de las tecnologías 5G[7], así como el papel transformador que el sector TIC en su conjunto, ha jugado en la innovación y rediseño de los modelos de negocio de todos los sectores en la denominada era digital, lo que le convierte en el catalizador que

[7] https://www.ericsson.com/4a68a4/assets/local/reports-papers/research-papers/how-5g-nr-can-reduce-network-energy-consumption.pdf

necesitan otros sectores para contribuir a la nueva economía de bajas emisiones de gases de efecto invernadero, ya que facilita usos innovadores de productos y servicios "inteligentes", ayudando a generar beneficios medioambientales y permitiendo ahorros de costes de energía a los usuarios.

Además, las telecomunicaciones son muy útiles en la tarea de supervisión ambiental y climática, incluido el pronóstico del tiempo, y fundamentales para las comunicaciones de alerta temprana y mitigación en caso de catástrofes.

Las conclusiones del estudio "Telecomunicaciones y CO2: El Papel de la Tecnología Móvil frente al Cambio Climático", indican que aplicando 13 iniciativas de la tecnología móvil se pueden reducir en 113 millones de toneladas las emisiones de CO2 (lo que equivale a las emisiones generadas por unos 50 millones de vehículos) y generar unos ahorros de energía de 43.000 millones de euros en Europa.

Para ello, se necesitarían 1.040 millones de nuevas conexiones móviles, de las cuales el 87% corresponderían a conexiones "máquina a máquina" (M2M).

Su aplicación en España implicaría una reducción de 10,6 millones de toneladas de emisiones de CO2 (equivale a las emisiones generadas por 4,7 millones de vehículos, que es el 15% del parque actual), y unos ahorros de energía de 4.042 millones de euros. En el caso español, se precisarían unos 98 millones de nuevas conexiones, de las cuales unos 85 millones serían conexiones M2M.

El ahorro energético se producirá principalmente tanto por ese mayor protagonismo de servicios inteligentes M2M (redes eléctricas inteligentes, logística inteligente, ciudades inteligentes y sistemas de producción inteligente) como por la sustitución de actividades físicas por otras virtuales.

Ese proceso de virtualización supondría la sustitución de procesos, desplazamientos, reuniones y viajes por alternativas virtuales de bajas emisiones. Se trataría, por ejemplo, de reducir los viajes apostando por salas de reuniones virtuales a las que conectarse a través de las telecomunicaciones, fomentar el uso de productos de telecomunicaciones para que los empleados puedan trabajar a distancia desde su casa o utilizar las comunicaciones móviles para mejorar los procesos de comercio electrónico y facilitar los sistemas de pedido y entrega de las compras. Estas iniciativas no solo permitirían adaptarnos a posibles medidas de contención sanitaria de posibles epidemias sino que al tiempo lograrían reducir las emisiones de CO2 en Europa en más de 22 millones de toneladas, así como un ahorro potencial en consumo energético de 14.100 millones de euros (en España: ahorros de 2 millones de toneladas de emisiones de CO2, y 1.330 millones de euros).

H. OTROS IMPACTOS

El proyecto de norma no tiene impacto en relación con la igualdad de oportunidades, la no discriminación y la accesibilidad universal de las personas con discapacidad.

No se aprecian tampoco impactos significativos del proyecto de norma en relación con la infancia la adolescencia y la familia**.**

I. DESCRIPCIÓN DE LA TRAMITACIÓN

De acuerdo con lo establecido 26.2 de la Ley 50/1997, de 27 de noviembre, del Gobierno, antes de la elaboración de la norma, se realizó a través de la sede electrónica del Ministerio de Asuntos Económicos y Transformación Digital, consulta pública previa que estuvo abierta hasta el día 13 de diciembre de 2019.

Asimismo, de acuerdo con lo establecido en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno, el anteproyecto será sometido a trámite de audiencia pública mediante su publicación en la citada sede electrónica.

El anteproyecto será sometido a dictamen del Consejo de Estado .

Finalmente, de conformidad con el artículo 26.4 de la Ley 50/1997, de 27 de noviembre, del Gobierno, posteriormente, el anteproyecto será elevado, previo sometimiento a la CGSEYS, al Consejo de Ministros para que este decida sobre los ulteriores trámites.

J. EVALUACIÓN EX POST

El anteproyecto no prevé mecanismos concretos de evaluación ex post.

Pero, de acuerdo con los artículos 25.2 de la Ley 50/1997, de 27 de noviembre y 3.2 del Real Decreto 286/2017, de 24 de marzo, por el que se regulan el Plan Anual Normativo y el Informe Anual de Evaluación Normativa de la Administración General del Estado y se crea la Junta de Planificación y Evaluación Normativa, esta Ley podría llegar a ser seleccionada para evaluación posterior.

En ese caso, habrá de evaluarse la eficacia de la norma, esto es, el grado de cumplimiento de los objetivos y fines de la norma, que son afianzar la seguridad de las redes y servicios 5G y conseguir una pronta adopción de la tecnología 5G en los sectores que más pueden beneficiarse de las ventajas derivadas de su gran ancho de banda y baja latencia.

Para evaluar el primer objetivo, podrían utilizarse como indicadores, el número de incidentes de seguridad en las redes 5G o en los servicios que las usen que se hayan notificado. Para evaluar el segundo, podría medirse por el número de aplicaciones desarrolladas o en preparación, el número de sectores a que corresponden y las mejoras o transformaciones digitales a que ha dado lugar.

Deberá atenderse a los criterios de evaluación que pudieran establecerse en eventuales normas o recomendaciones comunitarias, y contribuir a la evaluación comunitaria, si así se estableciera.