CUATRECASAS

TECNOLOGÍA Y
TELECOMUNICACIONES

Ciberseguridad y 5 G

Sombras jurídicas de la Propuesta de Reglamento sobre la Ciberseguridad 2 en materia de redes de comunicaciones electrónicas

España | Legal Flash | Marzo 2026

ASPECTOS CLAVE

- La Propuesta de Reglamento sobre la **Ciberseguridad 2** impone **restricciones** notables sobre las cadenas de suministro TIC relativas a las **redes de comunicaciones electrónicas**
- Las restricciones afectan a los **operadores** vinculados con países que planteen preocupaciones de ciberseguridad que se declaren **de alto riesgo**
- Los **componentes** de operadores de alto riesgo **no podrán ser usados** por entidades públicas o privadas en áreas críticas. **Se prohíbe su uso futuro** en redes de comunicaciones móviles, fijas y por satélite. Los **componentes actuales** deben **eliminarse en** el plazo de **36 meses.**
- La Propuesta de Reglamento sobre la **Ciberseguridad 2** colisiona con principios relevantes de Derecho de la Unión:
  - Principio de atribución (invasión de competencias estatales)
  - Principios de subsidiariedad y proporcionalidad
  - Principio de no discriminación por razón de nacionalidad y no discriminación tecnológica

La Propuesta de Reglamento sobre la Ciberseguridad 2

Al tiempo de redactar este "legal flash", se encuentra en tramitación la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la seguridad de la cadena de suministro TIC y por la que se deroga el Reglamento (UE) 2019/881, del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. º 526/2013 ("**Propuesta de Reglamento sobre la Ciberseguridad 2**").

Su **objeto** presenta **triple faz**:

- delimitar la misión, los objetivos, las tareas y las cuestiones organizativas relativas a la **Agencia de la Unión Europea para la Ciberseguridad** (ENISA);
- fijar un **marco** para el establecimiento de **esquemas europeos de certificación de la ciberseguridad**, con el fin de garantizar el nivel adecuado de ciberseguridad de los productos TIC, servicios TIC, procesos TIC, servicios de seguridad gestionados o la postura cibernética de las entidades de la Unión, así como con el fin de evitar la fragmentación del mercado interior en lo que respecta a los esquemas de certificación de ciberseguridad en la Unión; y,
- delimitar un **marco de cadena de suministro TIC** de confianza aplicable a las entidades públicas o privadas que presten servicios en los sectores de alta criticidad y otros sectores críticos regulados en los Anexos I y II de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad

La cadena de suministros TIC es la que se refiere a los productos , activos, servicios y procesos TIC; es decir, a los elementos de las redes o sistemas de información; a la transmisión, almacenamiento, recuperación o tratamiento de información por medio de sistemas de redes e información; al conjunto de actividades relacionadas con esos productos y servicios; y a activos de software o hardware en los sistemas de redes y de información.

Concierne, pues, al **ecosistema de las redes de telecomunicaciones** y, en particular, al **conjunto de componentes, elementos y servicios necesarios para el despliegue y utilización de las redes de telecomunicaciones 5G**.

Las restricciones a la cadena de suministros TIC. Impacto sobre el despliegue y utilización de redes 5 G

El aspecto de la Propuesta de Reglamento sobre la Ciberseguridad 2 que presenta un **mayor nivel de novedad**, una singularidad más relevante y, también, **mayores incertidumbres jurídicas** es, precisamente, el referido a **la cadena de suministros TIC.**

Su contenido es **fuertemente intervencionista**: impone un abanico de restricciones que **impactan** de una manera directa e inmediata sobre la prestación de **servicios de comunicaciones electrónicas** por parte de empresas o entidades de terceros Estados.

Estas restricciones recaen sobre los **operadores o proveedores de alto riesgo**, concepto que incluye a las empresas que suministran componentes TIC y componentes que incluyan componentes TIC establecidos en un **tercer país que plantee preocupaciones de ciberseguridad** para las cadenas de suministro TIC o controlados por dicho tercer país o por una entidad establecida en dicho tercer país o por una nacional del mismo.

Las **restricciones** son, en síntesis, las siguientes:

- Se **veta** la **participación** de **operadores o proveedores de alto riesgo** en **programas o instrumentos de financiación de la Unión** relacionados con el suministro de componentes TIC o componentes que incluyan componentes TIC para ser utilizados en activos TIC clave.
- Se **veta el uso de componentes TIC** o componentes que incluyan componentes TIC **suministrados por proveedores de alto riesgo** por parte de entidades públicas o privadas que presten servicios en sectores de alta criticidad y otros sectores críticos.
- Se ordena la **eliminación gradual**, en un periodo de tiempo inferior **a treinta y seis meses**, de los **componentes TIC** o de componentes que incluyan componentes TIC **suministrados por proveedores de alto riesgo** de los activos TIC clave de las redes de comunicaciones electrónicas móviles, fijas y por satélite; y,
- Se **prohíbe el uso, instalación o integración** en cualquier forma, por parte de los proveedores de redes de comunicaciones electrónicas móviles, fijas y por satélite, **de componentes TIC** o componentes que incluyan componentes TIC **de proveedores de alto riesgo** en el funcionamiento de activos TIC clave.

A nadie se le escapa la **consecuencia práctica** de estas restricciones: los **operadores o proveedores de alto riesgo** quedan sustancialmente **excluidos** —con efectos retroactivos, pues las restricciones afectan a componentes ya instalados— de los **despliegues de redes de comunicaciones** y, en particular, de las redes de comunicaciones **5G.**

Finalidad y antecedentes de las restricciones a la cadena de suministros TIC

Este efecto —la **exclusión de los operadores de alto riesgo provenientes de terceros Estados** del despliegue de redes de comunicaciones 5 G— es, nítidamente, el **objetivo perseguido por la Propuesta de Reglamento sobre la Ciberseguridad 2.** El Memorando Explicativo de la Propuesta, así como los considerandos de ésta, lo expone en sentido positivo, pero de forma que no deja lugar a dudas. Se pretende "*reforzar las cadenas de suministro TIC garantizando la soberanía tecnológica europea sobre activos clave, lo que aumentaría la resiliencia de la Unión y podría beneficiar los esfuerzos de ciberdefensa*" [Considerando (4)], de tal manera que se eviten "*incidentes de ciberseguridad a gran escala que afectan a infraestructuras críticas, servicios digitales o funciones sociales esenciales*" y que "*pueden tener impactos en la población que requieren una acción coordinada de Protección Civil y gestión de crisis a nivel de la Unión*" [Considerando (5)].

Este objetivo **se alinea con otras actuaciones previas de la Unión Europea** entre las que pueden citarse las Conclusiones del Consejo Europeo de 21 y 22 de marzo de 2019, en las que se solicitó una recomendación de la Comisión sobre un enfoque concertado de la seguridad de las redes 5 G; la Recomendación (UE) 2019/534, de la Comisión, de 26 de marzo de 2019, sobre ciberseguridad de las redes 5G; la Comunicación de la Comisión Europea de 29 de enero de 2020, "Despliegue seguro de la 5 G en la UE – Aplicación de la caja de herramientas de la UE" (COM/2020/50 final); o la Comunicación de la Comisión de 15 de junio de 2023, "Aplicación del conjunto de instrumentos de la UE para la seguridad de las redes".

Existe, no obstante, **una diferencia muy notable entre** la **Propuesta de Reglamento sobre la Ciberseguridad 2 y las actuaciones previas referidas al despliegue de las redes 5 G. Frente al** carácter de mera recomendación a los Estados miembros de estas últimas, con una naturaleza de **"soft law"** y una intromisión mínima de la Unión Europea en la soberanía de los Estados en materia de seguridad, **la Propuesta se sitúa justo en el otro extremo del espectro**: **utiliza como instrumento de intervención** el más riguroso de los incluidos en el arsenal del Derecho de la Unión: **el Reglamento**, acto legislativo de la Unión que posee un **efecto vinculante y obligatorio en todos sus elementos** y cuya entrada en vigor lo convierte automáticamente en una norma aplicable sin necesidad de transposición nacional.

La muy discutible regularidad jurídica de las restricciones a la cadena de suministros TIC

Soberanía estatal en materia de seguridad y principio de atribución

La mutación radical que supone sustituir los mecanismos de "soft law" del Derecho de la Unión por un instrumento normativo tan riguroso como el Reglamento permite que se susciten muy **serias dudas acerca de la competencia misma de la Unión para imponer restricciones a la cadena de suministros TIC** que resulten vinculantes para los Estados miembros.

En este sentido, conviene recordar que las competencias de la Unión Europea se rigen por el **principio de atribución**, que le permite actuar únicamente dentro de los límites de las competencias que le confieren los Estados miembros en los Tratados, de tal manera que las competencias no atribuidas en los Tratados corresponden a los Estados miembros (artículo 5 del Tratado de la Unión Europea).

Entre las competencias atribuidas a la Unión no se encuentra la de **seguridad**. Es, por el contrario, una manifestación esencial de la **soberanía estatal** y, en consecuencia, una **competencia irrestricta de los Estados miembros.** El artículo 4.2 del Tratado de la Unión Europea señala expresamente que la Unión debe respetar las funciones esenciales del Estado, entre las que enumera las relacionadas con la seguridad nacional que *"seguirá siendo responsabilidad exclusiva de cada Estado miembro"*. El Tribunal de Justicia de la Unión Europea[1] y el Tribunal Constitucional español (sentencias 10/2023, 20/2023, 36/2023 y 60/2023) han subrayado la competencia exclusiva de los Estados miembros en materia de seguridad.

Si se toma en consideración esta idea, y se repara en que **el régimen de restricciones a la cadena de suministros TIC** establecido por la Propuesta de Reglamento sobre la Ciberseguridad 2 está **inequívocamente conectado con la seguridad pública interior de los Estados miembros** —como se declara en los considerandos (133), (135), (137), (139), (140) y (152), la conclusión se alcanza con facilidad: la Propuesta de Reglamento infringe el principio de atribución al invadir competencias típicamente relacionadas con la soberanía estatal, como son las de seguridad nacional.

Esta conclusión se reconoce implícitamente por el Informe Especial del Tribunal de Cuentas Europeo 3/2022 (titulado "Despliegue de la tecnología 5 G en la UE: Retrasos en el despliegue de redes y problemas de seguridad que siguen sin resolverse"), así como por la respuesta de la Comisión a dicho Informe; y no se ve alterada por el hecho de que la Propuesta invoque el artículo 114 del Tratado de Funcionamiento de la Unión Europea como base jurídica de su aprobación. **La invocación de la competencia en materia de mercado interior** —que es la que se recoge en dicho precepto— **no es admisible porque no atribuye al legislador de la Unión una competencia general** para regular cualquier materia relacionada con el mercado interior, lo que sería contrario al principio de atribución (Sentencia del Tribunal de Justicia de la Unión Europea de 5 de octubre de 2000, Alemania/Parlamento y Consejo, C-376/98, Tobacco Advertising, ECLI:EU:C:2000:544).

Como tampoco se ve alterada por la jurisprudencia del Tribunal de Justicia relativa a la aplicación del Derecho de la Unión a las medidas de seguridad pública [sentencia del Tribunal de Justicia (Gran Sala) de 15 de diciembre de 2009, Comisión/Finlandia, recaída en el asunto C-284/05 (ECLI:EU:C:2009:778)] que solo significa que la competencia exclusiva estatal en materia de seguridad no puede emplearse como un subterfugio para eludir la aplicación de los principios y libertades de la Unión, pero que no entraña que la Unión disponga de una competencia propia en materia de seguridad pública que se superponga a la de los Estados.

Principios de proporcionalidad y subsidiariedad

La Propuesta de Reglamento sobre la Ciberseguridad 2 también suscita dudas jurídicas de calado en relación con los principios de proporcionalidad y subsidiariedad.

---

1 Sentencia del Tribunal de Justicia de la Unión Europea, de 5 de abril de 2022, Commissioner of An Garda Síochána y otros, C-140/20, ECLI:EU:C:2022:258, apartado 61 y jurisprudencia allí citada.

En lo que concierne al **principio de proporcionalidad**, no parece necesario detenerse en su significado y contenido, al haber sido reconocido expresamente en el artículo 5.4 del Tratado de la Unión Europea y al ser invocado con reiteración por el Tribunal de Justicia de la Unión Europea[2]. Pero sí es preciso destacar que las restricciones a las cadenas de suministro TIC incluidas en la Propuesta pueden entrañar una vulneración del principio de proporcionalidad desde un doble ángulo: (*i*) en la elección del instrumento normativo; y (*ii*) en el contenido material de la Propuesta.

En efecto, la elección del concreto tipo de acto a adoptar por el legislador de la Unión debe fundarse, de conformidad con el artículo 296 del TFUE, en el procedimiento aplicable y el principio de proporcionalidad. En la Propuesta de Reglamento sobre la Ciberseguridad 2, la elección de un reglamento resulta justificada por lo que se refiere a aquellas medidas que revisan y derogan las previsiones del Reglamento 2019/881, pues parece lógico que tal derogación se produzca por efecto de una norma del mismo tipo. Sin embargo, no sucede lo mismo con aquellas disposiciones del nuevo reglamento que se refieren a aspectos novedosos en la regulación porque las justificaciones ofrecidas por la Comisión (riesgos derivados del proceso de transposición en términos de falta de uniformidad, inseguridad jurídica o incluso riesgo de discriminación de las situaciones transfronterizas) resultan excesivamente genéricas y, lo que es más importante, podrían predicarse de cualquier directiva en cualquier materia. Cabe, pues, afirmar que existen dudas más que razonables acerca del respeto al principio de proporcionalidad en la **elección del instrumento normativo**.

Y otro tanto sucede con el **contenido material de la Propuesta,** ya que, en contra de lo exigido por el Tribunal de Justicia de la Unión (sentencia de España/Consejo, C-310/04, EU:C:2006:521), no se ha demostrado hasta el momento que el análisis de la proporcionalidad realizado se base en datos completos y correctos.

Tampoco resulta convincente la Propuesta de Reglamento sobre la Ciberseguridad 2 en lo que atañe al **principio de subsidiariedad.**

Este principio, que limita el ejercicio de las competencias compartidas por parte de la Unión Europea, exige que la intervención de la Unión se produzca "*solo en caso de que, y en la medida en que, los objetivos de la acción pretendida no puedan ser alcanzados de manera suficiente por los Estados miembros, ni a nivel central ni a nivel regional o local, sino que puedan alcanzarse mejor, debido a la dimensión o a los efectos de la acción pretendida, a escala de la Unión*" (artículo 5.3 TUE).

Pues bien, en la hipótesis de que nos halláramos efectivamente ante una competencia compartida, para respetar el principio de subsidiariedad **sería necesario que la Propuesta** de Reglamento sobre la Ciberseguridad 2 **hubiera acreditado debidamente** que los objetivos de la Propuesta no pueden ser alcanzados de manera suficiente por los Estados miembros (**juicio de necesidad**) y que la acción, debido a su dimensión o efectos, ha de poder realizarse con más éxito a escala de la Unión (**valor añadido**); algo que, a la vista de los trabajos preparatorios realizados hasta la fecha resulta cuando menos opinable.

Principios de no discriminación por razón de la nacionalidad y no discriminación tecnológica

La Propuesta de Reglamento sobre la Ciberseguridad 2 prevé la designación de terceros países que plantean preocupaciones de ciberseguridad, así como el establecimiento de listas de proveedores de alto riesgo a los que se aplicarán las restricciones a la cadena de suministros TIC. **No concreta**, sin embargo, qué países plantean problemas de ciberseguridad ni quiénes serán los **proveedores de alto riesgo**, ya que, en ambos casos, su delimitación se difiere a posteriores actos de ejecución de la Comisión. **No parece**, sin embargo, **difícil concretar quiénes serán** unos y otros, dado que la Comunicación de la Comisión de 15 de junio de 2023, sobre aplicación del conjunto de instrumentos de la UE para la seguridad de las redes se refiere de forma explícita a conocidos operadores del sector, pertenecientes a un país muy concreto: la República Popular China.

Esta circunstancia determina que, no tanto la propia Propuesta de Reglamento como sus actos de ejecución, puedan colisionar con uno de los más relevantes principios y derechos fundamentales del

---

2 Sentencia del Tribunal de Justicia de la Unión Europea de 12 de julio de 2001, Jippes y otros, C-189/01, EU:C:2001:420, apdo. 81.

ordenamiento jurídico español y los correspondientes al Derecho de la UE: la **prohibición de medidas discriminatorias por razón de la nacionalidad o el origen nacional** [artículo 14 de la Constitución, artículo 21 de la Carta de los Derechos Fundamentales y artículo 18 del Tratado de Funcionamiento de la Unión Europea; también, inter al., sentencia (Gran Sala) del Tribunal de Justicia de la Unión Europea de 27 de octubre de 2009, Asunto C-115/08 (ECLI:EU:C:2009:660)]. Máxime si se tiene en cuenta que el Reino de España y la República Popular China celebraron un acuerdo para la promoción y protección recíprocas de inversiones, en Madrid, el 14 de noviembre de 2005, que prohíbe expresamente cualquier forma de trato discriminatorio o diferenciado por razón de la nacionalidad, favoreciendo siempre un trato justo y equitativo.

Ello sin perjuicio de que el veto a productos y tecnologías de origen extraño a la Unión Europea también podría incurrir en la potencial infracción del principio de neutralidad tecnológica garantizado por la Directiva (UE) 2018/1972 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (refundición) y aplicado de manera reiterada por el Tribunal de Justicia de la Unión Europea [por ej., Sentencia de 15 de abril de 2021, Asunto C-515/19 (ECLI:EU:C:2021:273)].

Conclusión

La regulación de las cadenas de suministro TIC, en particular en lo que atañe a la imposición de restricciones a los denominados operadores o proveedores de alto riesgo presenta **dudas jurídicas de calado muy notable**. Algunas de ellas afectan a **principios clásicos muy conocidos** y aplicados en el ámbito de la Unión, como los de subsidiariedad, proporcionalidad y no discriminación. Pero **las dudas más intensas** se suscitan en torno a una cuestión medular y crítica: la propia competencia de la Unión Europea para adoptar medidas en materia de seguridad nacional y la **posible usurpación**, más allá del principio de atribución, de competencias típicamente estatales —la seguridad interior— fuertemente enraizadas con la **idea de soberanía.**

Para obtener información adicional sobre el contenido de este documento puede enviar un mensaje a nuestro equipo del Área de Conocimiento e Innovación o dirigirse a su contacto habitual en Cuatrecasas.