2023/2113

11.10.2023

RECOMENDACIÓN (UE) 2023/2113 DE LA COMISIÓN

de 3 de octubre de 2023

sobre ámbitos tecnológicos críticos para la seguridad económica de la UE con vistas a realizar evaluaciones de riesgos adicionales conjuntamente con los Estados miembros

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Considerando lo siguiente:

(1) La Comisión y el alto representante han reconocido que, con el aumento de las tensiones geopolíticas, la mayor integración económica y la aceleración del desarrollo tecnológico, determinados flujos y actividades económicos pueden presentar un riesgo para nuestra seguridad económica y han adoptado una Comunicación conjunta sobre la Estrategia Europea de Seguridad Económica ([1]) para establecer un enfoque estratégico global de la seguridad económica.

(2) La Estrategia Europea de Seguridad Económica se basa en un enfoque fundado en tres pilares: la promoción de la base económica y la competitividad de la UE; la protección frente a los riesgos; y la asociación con el mayor número posible de países para abordar preocupaciones e intereses comunes.

(3) En este contexto y en vista de los riesgos que pueden presentar determinadas dependencias económicas y evoluciones técnicas, la UE necesita tener una visión clara de los riesgos para su seguridad económica y de la evolución de estos a lo largo del tiempo.

(4) Estos riesgos deben ser determinados y evaluados conjuntamente con los Estados miembros de la UE, en un proceso dinámico y continuo que cuente con las aportaciones de las partes interesadas privadas.

(5) La Estrategia Europea de Seguridad Económica estableció las siguientes cuatro categorías de riesgos, amplias y no exhaustivas, con vistas a realizar evaluaciones adicionales: resiliencia de las cadenas de suministro, incluida la seguridad energética; seguridad física y ciberseguridad de las infraestructuras críticas; seguridad tecnológica y filtraciones de tecnología; utilización de las dependencias económicas como arma y coerción económica.

(6) En la Comunicación conjunta, la Comisión se comprometió a evaluar los riesgos de la seguridad tecnológica y de las filtraciones de tecnología sobre la base de una lista de tecnologías estratégicas críticas para la seguridad económica y, por lo que se refiere a los riesgos más sensibles, proponer una lista de tecnologías críticas con vistas a realizar una evaluación de riesgos que deberá llevarse a cabo colectivamente con los Estados miembros antes del final de 2023.

(7) La Comunicación conjunta estableció los siguientes tres criterios, estrictamente definidos y orientados al futuro, para la selección de las tecnologías que presentan los riesgos más sensibles, con vistas a realizar evaluaciones adicionales: el carácter facilitador y transformador de la tecnología; el riesgo de fusión del uso civil y militar; y el riesgo de uso indebido de la tecnología para cometer violaciones de los derechos humanos.

(8) El criterio relativo al carácter facilitador y transformador de la tecnología analiza el potencial y la relevancia de la tecnología para impulsar aumentos significativos del rendimiento y la eficiencia o cambios radicales en relación con los sectores, las capacidades, etc.

(9) El criterio relativo al riesgo de fusión del uso civil y militar analiza la relevancia de la tecnología para los sectores civil y militar y su potencial para hacer progresar estos dos ámbitos, así como el riesgo de que se utilicen determinadas tecnologías para comprometer la paz y la seguridad.

([1]) 20 final

(10) El criterio relativo al riesgo de uso indebido de la tecnología para cometer violaciones de los derechos humanos analiza el posible uso indebido de la tecnología en violaciones de los derechos humanos, incluida la restricción de las libertades fundamentales.

(11) Tras un primer análisis interno, la Comisión ha establecido una lista de diez ámbitos tecnológicos críticos para la seguridad económica de la UE. Esta lista de ámbitos tecnológicos tiene en cuenta el trabajo realizado en el marco del Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial ([2]). Se trata de un documento vivo y, como parte de un ejercicio en curso, podría ser objeto de nuevas modificaciones que reflejen los avances tecnológicos.

(12) Sobre la base de los tres criterios, estrictamente definidos y orientados al futuro, para la selección de tecnologías con vistas a realizar evaluaciones adicionales, la presente Recomendación señala cuatro ámbitos tecnológicos de la citada lista que considera muy probable que presenten los riesgos más sensibles e inmediatos relacionados con la seguridad tecnológica y las filtraciones de tecnología, a saber, los semiconductores avanzados, la inteligencia artificial, las tecnologías cuánticas y las biotecnologías. Como cuestión de máxima prioridad, estos ámbitos tecnológicos deben ser objeto de una evaluación de riesgos colectiva con los Estados miembros antes de que finalice el año. A reserva de la delimitación del alcance de los trabajos con los Estados miembros, esta evaluación colectiva podrá centrarse en subconjuntos de tecnologías que estén dentro de esos cuatro ámbitos tecnológicos.

(13) La estructuración de la lista refleja la evaluación de la Comisión acerca de cuáles, de entre los ámbitos tecnológicos que allí figuran, son los que tienen mayor probabilidad de presentar los riesgos más sensibles e inmediatos relacionados con la seguridad tecnológica y las filtraciones de tecnología. Esto puede servir de ayuda para la toma de decisiones en las próximas etapas. La Comisión entablará un diálogo abierto con los Estados miembros acerca del calendario y el alcance adecuados de las evaluaciones de riesgos adicionales, teniendo en cuenta, entre otras cosas, la contribución del factor temporal a la evolución de los riesgos. La Comisión agradecería que el intercambio sobre este aspecto de la Estrategia de Seguridad Económica en el Consejo se produjese en tiempo oportuno, en el marco de sus deliberaciones y orientaciones políticas generales en respuesta a la Comunicación conjunta. La Comisión podrá presentar nuevas iniciativas a este respecto a más tardar en primavera de 2024, a la luz de dicho diálogo y de la primera experiencia con las evaluaciones colectivas iniciales, así como de otras aportaciones que puedan recibirse sobre los ámbitos tecnológicos de la lista. A la hora de tomar decisiones para proponer evaluaciones de riesgos colectivas adicionales con los Estados miembros relativas a uno o varios de los otros ámbitos tecnológicos de la lista, o subconjuntos de estos, la Comisión tendrá en cuenta las acciones en curso o previstas que tienen por objeto promover el ámbito tecnológico considerado o crear asociaciones en este ámbito. En términos más generales, la Comisión tendrá en cuenta que las medidas adoptadas para aumentar la competitividad de la UE en los ámbitos pertinentes puedan contribuir a reducir determinados riesgos tecnológicos.

(14) El objetivo de la evaluación de riesgos debe ser detectar y analizar las vulnerabilidades de carácter sistémico en función de su posible impacto en la seguridad económica de la UE y del grado de probabilidad de que se materialice el impacto negativo. Con el fin de estructurar el próximo ejercicio de evaluación de riesgos con los Estados miembros, la Comisión ha definido algunos principios rectores.

(15) La presente Recomendación no predetermina el resultado de la evaluación de riesgos. Solo el resultado de la evaluación colectiva detallada del nivel y la naturaleza de los riesgos presentados puede servir de base para un nuevo debate sobre la necesidad de adoptar medidas precisas y proporcionadas para promover y proteger cualquiera de estos ámbitos tecnológicos, o cualquier subconjunto de estos, o crear asociaciones en esos ámbitos. Los Estados miembros y la Comisión podrán utilizar esta información para diseñar futuras acciones políticas, incluidas medidas de promoción, asociación o protección a escala nacional, de la UE o internacional, que deben ser proporcionales al nivel de riesgo afrontado y precisas en cuanto a su alcance. Por consiguiente, en esta fase de evaluación previa no puede extraerse ninguna conclusión con respecto al recurso a un instrumento concreto de las herramientas de la UE o de los Estados miembros para la promoción, la asociación con otros o la protección con vistas a una mayor seguridad económica.

(16) Cualquier medida que pueda adoptarse será proporcionada y estará dirigida con precisión a los riesgos evaluados de cada ámbito tecnológico crítico o de una tecnología concreta. Cualquier medida aplicada tendrá por objeto consolidar la fortaleza de la Unión en estos ámbitos y se diseñará para minimizar cualquier efecto indirecto negativo en el mercado y la economía. En particular, estas evaluaciones contribuirán al desarrollo de políticas de la Unión en apoyo de la innovación y el desarrollo industrial de las tecnologías señaladas, incluso a través de iniciativas internacionales.

([2]) 70 final

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

1. De la lista de diez ámbitos tecnológicos críticos enumerados en el anexo, se recomienda, como primer paso, que los Estados miembros, junto con la Comisión, evalúen, antes del final de 2023, los siguientes cuatro ámbitos tecnológicos que tienen la mayor probabilidad de presentar los riesgos más sensibles e inmediatos relacionados con la seguridad tecnológica y las filtraciones de tecnología:

   a) Tecnologías avanzadas de semiconductores

      Los semiconductores, la microelectrónica y la fotónica son componentes esenciales de los dispositivos electrónicos en ámbitos críticos como las comunicaciones, la computación, la energía, la salud, el transporte, la defensa y los sistemas y aplicaciones espaciales. Debido a su enorme carácter facilitador y transformador y a su uso con fines civiles y militares, mantenerse a la vanguardia de la construcción de estas tecnologías y seguir desarrollándolas es crucial para la seguridad económica.

   b) Tecnologías de inteligencia artificial

      La IA (*software*), la computación de alto rendimiento, la computación en la nube y periférica y el análisis de datos tienen una amplia gama de aplicaciones de doble uso y son cruciales, en particular, para tratar grandes cantidades de datos y tomar decisiones o realizar predicciones basadas en el análisis de esos datos. Estas tecnologías tienen un enorme potencial transformador en este sentido.

   c) Tecnologías cuánticas

      Las tecnologías cuánticas tienen un enorme potencial para transformar múltiples sectores, civiles y militares, al permitir que nuevas tecnologías y sistemas hagan uso de las propiedades de la mecánica cuántica. El impacto total de las tecnologías cuánticas que se están desarrollando o se desarrollarán todavía no puede determinarse en su totalidad.

   d) Biotecnologías

      Las biotecnologías tienen un carácter facilitador y transformador importante en ámbitos como la agricultura, el medio ambiente, la asistencia sanitaria, las ciencias biológicas, las cadenas alimentarias o la biofabricación. Algunas biotecnologías, como la ingeniería genética aplicada a patógenos o los compuestos nocivos producidos por la modificación genética de microorganismos, pueden tener una dimensión militar o de seguridad, en particular cuando se utilizan indebidamente.

2. La Comisión invita a los Estados miembros a participar en un diálogo abierto acerca de un calendario y un alcance adecuados para la evaluación de riesgos colectiva de los otros ámbitos tecnológicos enumerados en el anexo, o subconjuntos de estos, teniendo en cuenta el entorno geopolítico en rápida evolución y los diferentes grados de probabilidad de que las tecnologías de la lista presenten los riesgos más sensibles e inmediatos relacionados con la seguridad tecnológica y las filtraciones de tecnología.

3. Para estructurar el ejercicio colectivo de evaluación de riesgos, se han definido los siguientes principios rectores:

   a) Detectar y analizar las vulnerabilidades en función de su posible impacto en la seguridad económica de la UE y del grado de probabilidad de que se materialice el impacto negativo. El análisis debe determinar los principales tipos de amenazas y los principales actores implicados en ellas y tener en cuenta los factores geopolíticos cuando sea pertinente para evaluar la probabilidad de que haya impactos negativos. También debe tener en cuenta, entre otras cosas, la cadena de valor de las tecnologías, la evolución de los riesgos, así como los avances tecnológicos pertinentes, incluido cualquier punto crítico y cualquier futuro punto crítico previsto, información sobre la posición relativa de la UE en cada tecnología, incluidos los agentes clave y los elementos del liderazgo comparativo de la Unión; la interconectividad global del ecosistema de la tecnología, incluida la investigación y la cadena de suministro de la tecnología.

   b) En la fase de delimitación del alcance de la evaluación colectiva, debe tenerse en cuenta si la evaluación detallada se centrará en algunos de los subconjuntos de tecnologías más importantes.

   c) La evaluación de riesgos no será específica de cada país.

d) Dar prioridad a los riesgos que puedan tener efectos en toda la UE.

e) Asegurarse de que haya sinergias y complementariedades con los análisis existentes a escala de la UE y de los Estados miembros, para incorporarlos al proceso de evaluación de riesgos.

f) Tener en cuenta las aportaciones del sector privado.

4. Previa solicitud, la evaluación de riesgos colectiva garantizará la confidencialidad de las aportaciones recibidas de los Estados miembros o del sector privado. El documento final de los resultados de la evaluación de riesgos colectiva se clasificará adecuadamente.

5. Los Estados miembros y la Comisión deben llevar a cabo la evaluación haciendo uso de los foros existentes o, en caso necesario, de otros nuevos, para incluir a los expertos pertinentes, según se requiera para cada una de las tecnologías críticas.

6. La Comisión seguirá supervisando los avances tecnológicos y, en caso necesario, complementará la presente Recomendación proponiendo tecnologías adicionales con vistas a realizar evaluaciones adicionales.

Hecho en Estrasburgo, el 3 de octubre de 2023.

Por la Comisión
Thierry BRETON
Miembro de la Comisión

ANEXO

Lista de 10 ámbitos tecnológicos críticos para la seguridad económica de la UE

	Ámbito tecnológico	Tecnologías* * *Las tecnologías enumeradas de cada ámbito se consideran elementos centrales probables de la evaluación de riesgos, pero no son exhaustivas.*
1.	TECNOLOGÍAS AVANZADAS DE SEMICONDUCTORES	— Microelectrónica, incluidos los procesadores — Tecnologías fotónicas (incluido el láser de alta energía) — Chips de alta frecuencia — Equipos de fabricación de semiconductores con tamaños de nodo muy avanzados
2.	TECNOLOGÍAS DE INTELIGENCIA ARTIFICIAL	— Computación de alto rendimiento — Computación en la nube y periférica — Tecnologías de análisis de datos — Visión computerizada, procesamiento del lenguaje, reconocimiento de objetos
3.	TECNOLOGÍAS CUÁNTICAS	— Computación cuántica — Criptografía cuántica — Comunicaciones cuánticas — Detección cuántica y radar cuántico
4.	BIOTECNOLOGÍAS	— Técnicas de modificación genética — Nuevas técnicas genómicas — Genética dirigida — Biología sintética
5.	TECNOLOGÍAS AVANZADAS DE CONECTIVIDAD, DE NAVEGACIÓN Y DIGITALES	— Comunicaciones y conectividad digitales seguras, como la red de acceso radio (RAN) y la Open RAN, o la 6G — Tecnologías de ciberseguridad, incluida la cibervigilancia, los sistemas de seguridad y de intrusión, la criminalística digital — Internet de las cosas y realidad virtual — Tecnologías de registros distribuidos y de identidad digital — Tecnologías de guiado, navegación y control, incluida la aviónica y el posicionamiento marino
6.	TECNOLOGÍAS AVANZADAS DE DETECCIÓN	— Detección electroóptica, mediante radar, química, biológica, radiológica y distribuida — Magnetómetros, gradiómetros magnéticos — Sensores de campos eléctricos subacuáticos — Gravímetros y gradiómetros de gravedad
7.	TECNOLOGÍAS ESPACIALES Y DE PROPULSIÓN	— Tecnologías específicas centradas en el espacio, desde el nivel de componente hasta el nivel de sistema — Tecnologías de vigilancia espacial y observación de la Tierra — Posicionamiento, navegación y temporización (PNT) espacial — Comunicaciones seguras, incluida la conectividad de órbita terrestre baja (LEO) — Tecnologías de propulsión, incluida la hipersónica y los componentes para uso militar

	Ámbito tecnológico	Tecnologías* * *Las tecnologías enumeradas de cada ámbito se consideran elementos centrales probables de la evaluación de riesgos, pero no son exhaustivas.*
8.	TECNOLOGÍAS ENERGÉTICAS	— Tecnologías de fusión nuclear, reactores y generación de energía, tecnologías de conversión radiológica/enriquecimiento/reciclado — Hidrógeno y nuevos combustibles — Tecnologías de cero emisiones netas, incluida la energía fotovoltaica — Redes inteligentes y almacenamiento de energía, baterías
9.	ROBÓTICA Y SISTEMAS AUTÓNOMOS	— Drones y vehículos (aéreos, terrestres, de superficie y subacuáticos) — Robots y sistemas de precisión controlados por robots — Exoesqueletos — Sistemas basados en la IA
10.	TECNOLOGÍAS AVANZADAS DE MATERIALES, DE FABRICACIÓN Y DE RECICLADO	— Tecnologías de nanomateriales, materiales inteligentes, materiales cerámicos avanzados, materiales de sigilo, materiales seguros y sostenibles desde el diseño — Fabricación aditiva, incluso en los trabajos de campo — Fabricación de microprecisión controlada digitalmente y mecanizado/soldadura con láser a pequeña escala — Tecnologías de extracción, procesamiento y reciclado de materias primas fundamentales (incluida la extracción hidrometalúrgica, la biolixiviación, la filtración nanotecnológica, el procesamiento electroquímico y la masa negra)