Jornal Oficial
da União Europeia

PT
Série L

2023/2113

11.10.2023

RECOMENDAÇÃO (UE) 2023/2113 DA COMISSÃO

de 3 de outubro de 2023

relativa a domínios tecnológicos críticos para a segurança económica da UE, visando a realização de uma nova avaliação dos riscos com os Estados-Membros

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

(1) A Comissão e o alto representante reconheceram que, com o aumento das tensões geopolíticas, o aprofundamento da integração económica e a aceleração do desenvolvimento tecnológico, determinados fluxos e atividades económicas podem constituir um risco para a nossa segurança económica e adotaram uma comunicação conjunta sobre a Estratégia Europeia em Matéria de Segurança Económica ([1]), para pôr em prática uma abordagem estratégica global da segurança económica.

(2) A Estratégia Europeia em Matéria de Segurança Económica assenta numa abordagem com três pilares: promoção da base económica e da competitividade da UE; proteção contra riscos; e parcerias com o maior número possível de países para dar resposta a preocupações e interesses comuns.

(3) No âmbito deste quadro e tendo em conta os riscos que certas dependências económicas e evoluções técnicas podem representar, a UE necessita de uma visão clara dos riscos para a sua segurança económica e da sua evolução ao longo do tempo.

(4) Estes riscos devem ser identificados e avaliados em conjunto com os Estados-Membros da UE, com contributos de partes interessadas privadas, num processo dinâmico e contínuo.

(5) A Estratégia Europeia em Matéria de Segurança Económica identificou as seguintes quatro categorias alargadas e não exaustivas de riscos merecedoras de avaliação mais aprofundada: segurança física e cibersegurança das infraestruturas críticas; segurança tecnológica e fuga de tecnologias; utilização de dependências económicas como arma e coerção económica.

(6) Na comunicação conjunta, a Comissão comprometeu-se a avaliar os riscos de segurança tecnológica e fuga de tecnologias com base numa lista de tecnologias estratégicas críticas para a segurança económica e, no que diz respeito aos riscos mais sensíveis, a propor uma lista de tecnologias críticas com vista a uma avaliação dos riscos a realizar coletivamente com os Estados-Membros até ao final de 2023.

(7) A comunicação conjunta identificou os seguintes três critérios estritamente definidos e prospetivos para a seleção das tecnologias que apresentam os riscos mais sensíveis, para avaliação mais aprofundada: a natureza facilitadora e transformadora de uma tecnologia; o risco de fusão civil-militar; e o risco de utilização abusiva da tecnologia para violações dos direitos humanos.

(8) O caráter facilitador e transformador do critério tecnológico analisa o potencial e a relevância que uma tecnologia tem para impulsionar aumentos significativos do desempenho e da eficiência e/ou mudanças radicais para setores, capacidades, etc.

(9) O critério do risco de fusão civil-militar analisa a relevância da tecnologia para os setores civil e militar e o seu potencial de fazer avançar ambos os domínios, bem como o risco de utilização de determinadas tecnologias para minar a paz e a segurança.

([1]) JOIN(2023) 20 final.

(10) O risco de utilização abusiva da tecnologia para violações dos direitos humanos tem em conta a potencial utilização abusiva da tecnologia em violação dos direitos humanos, incluindo a restrição das liberdades fundamentais.

(11) Na sequência de uma primeira análise interna, a Comissão identificou uma lista de dez domínios tecnológicos críticos para a segurança económica da UE. Esta lista de domínios tecnológicos tem em conta o trabalho realizado no âmbito do Plano de Ação sobre as sinergias entre as indústrias civis, da defesa e do espaço ([2]). A lista é um documento dinâmico, que poderá ser objeto de novas alterações que reflitam a evolução tecnológica no âmbito de um exercício em curso.

(12) Com base nos três critérios estritamente definidos e prospetivos para a seleção de tecnologias para uma avaliação mais aprofundada, a presente recomendação identifica nesta lista quatro domínios tecnológicos que considera altamente suscetíveis de apresentarem os riscos mais sensíveis e imediatos relacionados com a segurança tecnológica e a fuga de tecnologias, nomeadamente os semicondutores avançados, a inteligência artificial, as tecnologias quânticas e as biotecnologias. Estes domínios tecnológicos devem, com a máxima prioridade, ser objeto de uma avaliação coletiva dos riscos com os Estados-Membros até ao final do ano. Sob reserva de trabalhos exploratórios com os Estados-Membros, esta avaliação coletiva pode centrar-se em subconjuntos de tecnologias pertencentes a estes quatro domínios tecnológicos.

(13) A estruturação da lista reflete a avaliação da Comissão de quais domínios tecnológicos, entre os enumerados, são mais suscetíveis de apresentar os riscos mais sensíveis e imediatos relacionados com a segurança tecnológica e a fuga de tecnologias. Esta avaliação pode contribuir para a tomada de decisões sobre outras medidas. A Comissão encetará um diálogo aberto com os Estados-Membros sobre o calendário e o âmbito adequados de novas avaliações dos riscos, tendo em conta, nomeadamente, o contributo do fator temporal para a evolução dos riscos. A Comissão acolheria favoravelmente um diálogo atempado no Conselho sobre este aspeto da estratégia em matéria de segurança económica, no contexto das suas deliberações e orientações políticas gerais em resposta à comunicação conjunta. A Comissão pode apresentar outras iniciativas a este respeito até à primavera de 2024, à luz desse diálogo e da primeira experiência adquirida com as avaliações coletivas iniciais, bem como de outros contributos que possam ser recebidos sobre os domínios tecnológicos enumerados. Ao tomar decisões sobre propostas de novas avaliações coletivas dos riscos com os Estados-Membros sobre um ou mais dos domínios tecnológicos adicionais enumerados, ou seus subconjuntos, a Comissão terá em conta as ações em curso ou previstas para promover ou estabelecer parcerias no domínio tecnológico em causa. De um modo mais geral, a Comissão terá em conta que as medidas tomadas para reforçar a competitividade da UE nos domínios relevantes podem contribuir para reduzir determinados riscos tecnológicos.

(14) O objetivo da avaliação dos riscos deve ser identificar e analisar as vulnerabilidades de natureza sistémica em função do seu potencial impacto na segurança da economia da UE e do grau de probabilidade de o impacto negativo se concretizar. Para estruturar o futuro exercício de avaliação dos riscos com os Estados-Membros, a Comissão identificou alguns princípios orientadores.

(15) A presente recomendação não condiciona o resultado da avaliação dos riscos. Apenas o resultado da avaliação coletiva pormenorizada do nível e da natureza dos riscos apresentados pode servir de base para um debate mais aprofundado sobre a necessidade de quaisquer medidas precisas e proporcionadas de promoção, parcerias ou proteção em qualquer destes domínios tecnológicos, ou em qualquer subconjunto dos mesmos. Os Estados--Membros e a Comissão podem utilizar estas informações na conceção de futuras ações políticas, incluindo medidas de promoção, parcerias ou proteção a nível nacional, da UE ou internacional, que devem ser proporcionais ao nível de risco abordado e precisas em termos de âmbito. Por conseguinte, não é possível tirar qualquer conclusão nesta fase de pré-avaliação sobre o recurso a qualquer instrumento específico da UE ou dos Estados-Membros para promoção, parcerias ou proteção com terceiros, tendo em vista o reforço da segurança económica.

(16) Quaisquer medidas que possam ser tomadas serão proporcionais e orientadas com precisão para os riscos avaliados de cada domínio tecnológico crítico, ou de uma tecnologia relevante. Quaisquer medidas aplicadas visarão reforçar a força da União nestes domínios e serão concebidas de modo a minimizar quaisquer efeitos indiretos negativos sobre o mercado e a economia. Em especial, estas avaliações contribuirão para o desenvolvimento de políticas da União de apoio à inovação e ao desenvolvimento industrial das tecnologias identificadas, nomeadamente através de iniciativas internacionais,

([2]) COM(2021) 70 final.

ADOTOU A PRESENTE RECOMENDAÇÃO:

1. Da lista de dez domínios tecnológicos críticos identificados no anexo, recomenda-se, numa primeira fase, que os Estados-Membros, juntamente com a Comissão, avaliem, até ao final de 2023, os seguintes quatro domínios tecnológicos com maior probabilidade de apresentarem os riscos mais sensíveis e imediatos relacionados com a segurança tecnológica e a fuga de tecnologias:

   a) Tecnologias avançadas de semicondutores

      Os semicondutores, a microeletrónica e a fotónica são componentes essenciais dos dispositivos eletrónicos em domínios críticos como as comunicações, a computação, a energia, a saúde, os transportes e os sistemas e aplicações da defesa e do espaço. Devido à sua enorme natureza facilitadora e transformadora e à sua utilização para fins civis e militares, continuar na vanguarda da criação e do desenvolvimento destas tecnologias é crucial para a segurança económica.

   b) Tecnologias de inteligência artificial

      A IA (*software*), a computação de alto desempenho, a computação em nuvem e periférica e a análise de dados têm uma vasta gama de aplicações de dupla utilização e são cruciais, em especial para o tratamento de grandes quantidades de dados e para tomar decisões ou fazer previsões assentas nesta análise baseada em dados. Estas tecnologias têm um enorme potencial transformador neste aspeto.

   c) Tecnologias quânticas

      As tecnologias quânticas têm um vasto potencial para transformar vários setores, civis e militares, permitindo novas tecnologias e sistemas que fazem uso das propriedades da mecânica quântica. O impacto total das tecnologias quânticas que estão a ser ou serão desenvolvidas ainda não pode ser plenamente qualificado.

   d) Biotecnologias

      As biotecnologias têm uma importante natureza facilitadora e transformadora em domínios como a agricultura, o ambiente, os cuidados de saúde, as ciências da vida, as cadeias alimentares ou o biofabrico. Algumas biotecnologias, como a engenharia genética aplicada a agentes patogénicos ou compostos nocivos produzidos pela modificação genética de microrganismos, podem ter uma dimensão de segurança ou militar, em especial quando são utilizadas de forma abusiva.

2. A Comissão convida os Estados-Membros a encetarem um diálogo aberto sobre um calendário e um âmbito adequados para a avaliação coletiva dos riscos dos outros domínios tecnológicos enumerados no anexo, tendo em conta o contexto geopolítico em rápida evolução e os diferentes graus de probabilidade de as tecnologias enumeradas apresentarem os riscos mais sensíveis e imediatos relacionados com a segurança tecnológica e a fuga de tecnologias.

3. Para estruturar o exercício de avaliação coletiva dos riscos, identificaram-se os seguintes princípios orientadores:

   a) Identificar e analisar as vulnerabilidades em função do seu potencial impacto na segurança económica da UE e do grau de probabilidade de o impacto negativo se concretizar. A análise deve identificar os principais tipos de ameaças e de intervenientes e ter em conta fatores geopolíticos, se for caso disso, para avaliar a probabilidade de impactos negativos. A análise deve também identificar, nomeadamente, a cadeia de valor das tecnologias, a evolução dos riscos bem como a evolução tecnológica pertinente, incluindo pontos de estrangulamento atuais e futuros, um levantamento da posição relativa da UE em cada tecnologia, incluindo os principais intervenientes e elementos da liderança comparativa da UE; a interconectividade global do ecossistema da tecnologia, incluindo na investigação e na cadeia de abastecimento da tecnologia;

   b) Na fase de delimitação do âmbito da avaliação coletiva, deve ter-se em conta se a avaliação pormenorizada se centrará em determinados subconjuntos de tecnologias mais relevantes;

   c) A avaliação dos riscos não será específica por país;

d) Dar prioridade aos riscos com efeitos potenciais em toda a UE;

e) Assegurar sinergias e complementaridades com as análises existentes a nível da UE e dos Estados-Membros, de modo a contribuir para o processo de avaliação dos riscos;

f) Ter em conta os contributos do setor privado.

4. A avaliação coletiva dos riscos deve assegurar a confidencialidade, mediante pedido, dos contributos recebidos dos Estados-Membros ou do setor privado. O documento final com os resultados da avaliação coletiva dos riscos deve ser classificado de forma adequada.

5. A avaliação deve ser realizada pelos Estados-Membros e pela Comissão, recorrendo aos fóruns existentes ou, se necessário, a novos fóruns para incluir especialistas relevantes, conforme o exigido para cada uma das tecnologias críticas.

6. A Comissão continuará a acompanhar a evolução tecnológica e, se necessário, complementará a presente recomendação, propondo tecnologias adicionais para uma avaliação mais aprofundada.

Feito em Estrasburgo, em 3 de outubro de 2023.

Pela Comissão
Thierry BRETON
Membro da Comissão

ANEXO

Lista de dez tecnologias críticas para a segurança económica da UE

	Domínio tecnológico	Tecnologias* * *As tecnologias enumeradas para cada domínio são pontos focais prováveis para a avaliação dos riscos, mas não são exaustivas*
1.	TECNOLOGIAS AVANÇADAS DE SEMICONDUTORES	— Microeletrónica, incluindo processadores — Tecnologias fotónicas (incluindo *laser* de alta energia) — Circuitos integrados de alta frequência — Equipamento de fabrico de semicondutores com dimensões de nós muito avançadas
2.	TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL	— Computação de alto desempenho — Computação em nuvem e periférica — Tecnologias de análise de dados — Visão computacional, processamento de linguagem, reconhecimento de objetos
3.	TECNOLOGIAS QUÂNTICAS	— Computação quântica — Criptografia quântica — Comunicações quânticas — Teledeteção e radar quânticos
4.	BIOTECNOLOGIAS	— Técnicas de modificação genética — Novas técnicas genómicas — Genética dirigida — Biologia sintética
5.	TECNOLOGIAS AVANÇADAS DE CONECTIVIDADE, NAVEGAÇÃO E DIGITAIS	— Comunicações digitais e conectividade seguras, tais como RAN e Open RAN (Rede de Acesso Rádio) e 6G — Tecnologias de cibersegurança, incluindo cibervigilância, sistemas de segurança e interferência, informática forense — Internet das coisas e realidade virtual — Tecnologias de registo distribuído e de identidade digital — Tecnologias de orientação, navegação e controlo, incluindo avió-nica e o posicionamento marítimo
6.	TECNOLOGIAS AVANÇADAS DE TELEDETEÇÃO	— Teledeteção eletro-ótica, por radar, química, biológica, radiológica e distribuída — Magnetómetros, gradiómetros magnéticos — Sensores de campo elétrico subaquáticos — Gravímetros e gradiómetros
7.	TECNOLOGIAS ESPACIAIS E DE PROPULSÃO	— Tecnologias específicas centradas no espaço, do nível de compo-nentes até ao nível de sistemas — Tecnologias de vigilância espacial e de observação da Terra — Posicionamento, navegação e sincronização espaciais — Comunicações seguras, incluindo conectividade em órbita terrestre de baixa altitude (LEO) — Tecnologias de propulsão, incluindo tecnologia hipersónica e com-ponentes para uso militar

	Domínio tecnológico	Tecnologias* * *As tecnologias enumeradas para cada domínio são pontos focais prováveis para a avaliação dos riscos, mas não são exaustivas*
8.	TECNOLOGIAS ENERGÉTICAS	— Tecnologias de fusão nuclear, reatores e produção de energia, tecnologias radiológicas de conversão/enriquecimento/reciclagem — Hidrogénio e novos combustíveis — Tecnologias de impacto zero, incluindo energia fotovoltaica — Redes inteligentes e armazenamento de energia, baterias
9.	ROBÓTICA E SISTEMAS AUTÓNOMOS	— Drones e veículos (aéreos, terrestres, de superfície e submarinos) — Robôs e sistemas de precisão controlados por robôs — Exoesqueletos — Sistemas baseados em IA
10.	TECNOLOGIAS AVANÇADAS DE MATERIAIS, FABRICO E RECICLAGEM	— Tecnologias para nanomateriais, materiais inteligentes, materiais cerâmicos avançados, materiais furtivos, materiais seguros e sustentáveis desde a conceção — Fabricação aditiva, incluindo no terreno — Fabrico de microprecisão de controlo digital e maquinagem/soldadura por *laser* em pequena escala — Tecnologias de extração, transformação e reciclagem de matérias-primas críticas (incluindo extração hidrometalúrgica, biolixiviação, filtração à base de nanotecnologias, processamento eletroquímico e massa negra)