Parlement européen
2024-2029

Commission de l'industrie, de la recherche et de l'énergie

2025/2007(INI)

25.2.2025

PROJET DE RAPPORT

sur la souveraineté technologique européenne et les infrastructures numériques (2025/2007(INI))

Commission de l'industrie, de la recherche et de l'énergie

Rapporteure: Sarah Knafo

SOMMAIRE

Page

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur la souveraineté technologique européenne et les infrastructures numériques (2025/2007(INI))

Le Parlement européen,

– vu le Traité sur l'Union européenne (TUE) et, plus particulièrement, son article 4,

– vu le Traité sur le Fonctionnement de l'Union européenne (TFUE), notamment ses articles 173, 179 et 190,

– vu la communication COM (2021) 118 de la Commission du 9 mars 2021 intitulée « *Une boussole numérique pour 2030 : la voie européenne pour la décennie numérique* »,

– vu la présentation de la Commission du 29 janvier 2025 pour une Boussole de compétitivité pour l'UE,

– vu le règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs (« *European Chips Act* »),

– vu la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive NIS 2),

– vu le rapport étendu « *Menaces prospectives en matière de cybersécurité pour 2030 - mise à jour 2024* » de l'Agence de l'UE pour la cybersécurité (ENISA),

– vu le règlement (UE) 2024/2847 du 23 octobre 2024 relatif aux exigences en matière de cybersécurité horizontales pour les produits comportant des éléments numériques,

– vu la proposition de règlement UE 2023/0109 (COD) présentée par la Commission le 18 avril 2023 visant à renforcer la solidarité de l'UE et ses capacités de détection, de préparation et de réaction face aux menaces et aux incidents de cybersécurité (Cyber Solidarity Act),

– vu la proposition de règlement UE 2023/0108 (COD) présentée par la Commission le 18 avril 2023 concernant les services de sécurité gérés (Cybersecurity Act),

– vu le Livre blanc de la Commission européenne du 21 février 2024 intitulé « *Comment maîtriser les besoins de l'Europe en matière d'infrastructures et réseaux de communication de l'UE ?* »,

– vu le règlement (UE) 2023/606 du Parlement européen et du Conseil du 15 mars 2023 modifiant le règlement (UE) 2015/760 en ce qui concerne les exigences relatives aux politiques d'investissement et aux conditions de fonctionnement des fonds européens d'investissement à long terme et la définition des actifs éligibles à l'investissement, les obligations en matière de composition et de diversification du portefeuille et l'emprunt

de liquidités et d'autres dispositions des statuts des fonds (Texte présentant de l'intérêt pour l'EEE),

– vu le rapport de M. Draghi, « *The future of European competitiveness (Part A | A competitiveness strategy for Europe* », septembre 2024,

– vu le rapport de M. Letta, « *More than a Market - Speed, security, solidarity - Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens* », avril 2024,

– vu la Communication du 2 juillet 2024 de la Commission européenne au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « *rapport 2024 sur l'état d'avancement de la décennie numérique* »,

– vu la recommandation de la GSM Association dans son rapport « *The Mobile Economy Europe 202*5 »,

– vu le *Clarifying Lawful Overseas Use of Data Act* (« *Cloud Act* ») américain, adopté en 2018,

– vu le *Foreign Intelligence Surveillance Act (« FISA* ») américain, adopté en 1978,

– vu le *Buy American Act* et *le Small business Act* américains,

– vu le *Executive Order 13771, « Reducing Regulation and Controlling Regulatory Costs* » (« *One-In, Two-Out* »), signé le 30 janvier 2017 aux États-Unis et révoqué le 20 janvier 2021,

– vu la directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II),

– vu la directive (UE) 2016/2341 du Parlement européen et du Conseil du 14 décembre 2016 concernant les activités et la surveillance des institutions de retraite professionnelle (IORP II),

– vu l'article 4 paragraphe 2 de la directive 2011/96/UE du Conseil du 30 novembre 2011 concernant le régime fiscal commun applicable aux sociétés mères et filiales d'États (directive dite mère-fille),

– vu le règlement (UE) 2019/943 du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité,

– vu le règlement (CE) n° 139/2004 du Conseil adopté le 20 janvier 2004 sur les concentrations d'entreprises,

– vu la Communication de la Commission européenne sur les critères relatifs à l'analyse de la compatibilité avec le marché intérieur des aides d'État destinées à promouvoir la réalisation de projets importants d'intérêt européen commun (PIIEC) 2021/C 528/02,

– vu le rapport de l'EPRS rédigé par M. Guillaume Ragannaud, « *The EU chips act: Securing Europe's supply of semiconductors* », juin 2023,

– vu l'article 55 de son règlement intérieur,

– vu le rapport de la commission de l'industrie, de la recherche et de l'énergie (A10-0000/2025),

A. considérant que la souveraineté technologique désigne notre capacité à maîtriser les technologies stratégiques nécessaires à notre indépendance économique, sécuritaire et politique ;

B. considérant que l'Union européenne (UE) dépend massivement d'infrastructures développées et contrôlées par des puissances étrangères, notamment les États-Unis ou l'Asie, ce qui fragilise sa compétitivité, expose ses données sensibles et limite sa capacité d'action stratégique ;

C. considérant que 92 % des données occidentales sont stockées aux États-Unis[1], que 69 % des parts de marché européen du *cloud* sont détenues par des acteurs américains[2], contre seulement 13 % pour les acteurs européens[3], ce qui expose les données européennes à des législations extraterritoriales, notamment la loi Fisa et le *Cloud Act* américain ;

D. considérant que l'UE ne représente que 7 % des investissements mondiaux en intelligence artificielle (IA), bien en deçà des États-Unis (40 %) et de la Chine (32 %[4]) ;

E. considérant que les récentes pénuries mondiales de semi-conducteurs ont entraîné des fermetures d'usines ; que la part de l'Union dans la production mondiale de puces électroniques n'est que de 10 % ;

F. considérant que les réseaux de fibre optique n'atteignent qu'environ 64 % des ménages[5], tandis que les réseaux 5G « de haute qualité » ne couvrent que 50 % du territoire de l'UE[6] ;

G. considérant qu'en 2020, une entreprise sur huit a été touchée par des cyberattaques[7] et qu'en 2023, ce chiffre atteindrait, selon le rapport Hiscox, 58 % en Allemagne et 53 % en France ;

H. considérant que les coûts énergétiques élevés de fonctionnement des infrastructures numériques pénalisent les acteurs européens ;

I. considérant que la commande publique représente un outil stratégique pour soutenir la recherche & développement (R&D) et les acteurs européens dans des secteurs clés comme le *cloud*, la cybersécurité, l'IA, les semi-conducteurs et les infrastructures de communication ;

[1] https://www.redes-sociales.com/wp-content/uploads/2020/11/european-digital-sovereignty_oliver-wyman.pdf
[2] Estimations du cabinet Synergy Research Group, 2022.
[3] https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share
[4] https://www.oecd.org/en/publications/venture-capital-investments-in-artificial-intelligence_f97beae7-en.html
[5] https://digital-strategy.ec.europa.eu/fr/news/eu39-reaches-70-ftthb-coverage-according-ftth-council-europe
[6] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52024DC0260
[7] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020JC0018

J. considérant que dans un marché fragmenté, de nombreuses entreprises européennes peinent à offrir des solutions compétitives à l'échelle mondiale face aux géants internationaux ;

K. considérant qu'en dispersant de petites subventions publiques sur trop de projets différents, l'UE ne permet à aucun d'atteindre une véritable masse critique ;

L. considérant que des incitations financières et fiscales favorisent les investissements de fonds privés ;

1. rappelle que la souveraineté technologique est un pilier fondamental pour la compétitivité, la sécurité et l'indépendance stratégique de l'UE ;

2. constate que la dépendance massive aux technologies étrangères expose l'Europe à des risques majeurs, notamment juridiques, économiques et sécuritaires ;

3. s'inquiète du fait que les entreprises européennes peinent à concurrencer les entreprises américaines et chinoises dans des secteurs stratégiques tels que le *cloud*, la cybersécurité, l'IA, les semi-conducteurs et les infrastructures de communication ;

4. déplore que les réglementations européennes alourdissent les charges administratives et les coûts pour les entreprises locales sans contrecarrer efficacement la domination des géants étrangers ;

5. réaffirme que les données sensibles doivent être hébergées sur des infrastructures souveraines, protégées des lois extraterritoriales étrangères ;

6. souligne l'urgence de réformer le fonctionnement des marchés publics européens pour permettre aux États membres de réserver leurs marchés stratégiques aux entreprises européennes respectant des critères de souveraineté ;

7. invite la Commission à aligner le niveau de certification le plus élevé (niveau « High ») du schéma de certification européen de cybersécurité pour les services *cloud* (EUCS), toujours en cours de discussion, sur les exigences de la certification SecNumCloud, afin de s'assurer que l'hébergeur ne soit pas soumis à une législation extra-européenne ;

8. invite la Commission à faciliter le déploiement de la 5G[8] en assouplissant les conditions de concentration d'entreprises, afin d'encourager la mutualisation des infrastructures ;

9. invite la Commission et les commissions compétentes du Parlement européen à promouvoir les partenariats publics-privés et à faciliter l'accès des entreprises technologiques européennes aux financements privés ;

10. invite la Commission et les commissions compétentes du Parlement à permettre aux assurances vie et aux fonds de pension d'investir dans les secteurs stratégiques et émergents, tels que le *cloud*, la cybersécurité, l'IA, les semi-conducteurs, en allégeant la réglementation qui rend les actifs risqués moins attractifs via des exigences de capital élevées et qui impose un principe de prudence trop strict ;

[8] *Rapport « The Mobile Economy Europe 2025 »*

11. invite la Commission et les commissions compétentes du Parlement européen à réviser le cadre juridique des Projets Importants d'Intérêt Européen Commun (PIIEC), afin d'y inclure des dérogations pour les fusions et acquisitions stratégiques lorsqu'un projet répond à un enjeu de souveraineté ;

12. invite la Commission à supprimer deux réglementations pour chaque nouvelle réglementation créée dans les secteurs stratégiques, à l'instar du décret américain « *One-In, Two-Out* » ;

13. invite la Commission à réformer le marché européen de l'électricité en mettant fin au mécanisme de l'ordre de mérite, qui aligne les prix sur les sources les plus chères, et en rétablissant un cadre permettant au nucléaire de fournir une électricité compétitive et stable ;

14. charge son Président de transmettre la présente résolution au Conseil et à la Commission.

EXPOSÉ DES MOTIFS

L'Union européenne (UE) est aujourd'hui fortement dépendante de technologies étrangères. Cela réduit sa capacité d'action stratégique et sa compétitivité économique. Cela expose aussi ses données sensibles, notamment du fait des lois extraterritoriales américaines. Cette situation pourrait perdurer avec les ambitions de la nouvelle administration Trump qui annonce 500 milliards de dollars dans le secteur clé de l'intelligence artificielle (IA) d'ici 2029.

Pourtant, l'UE dispose d'atouts indéniables, d'une forte capacité de recherche et d'un écosystème de start-ups et d'entreprises innovantes, comme l'a mis en lumière le Sommet de l'IA de Paris, en février 2025.

Ce rapport analyse les principales faiblesses dans les infrastructures stratégiques européennes. Il présente ensuite des recommandations pour parvenir rapidement à une souveraineté technologique fondée sur la compétitivité et la protection des marchés stratégiques.

Les concepts de souveraineté technologique européenne et d'infrastructures numériques

La souveraineté technologique vise à garantir notre indépendance et notre sécurité en protégeant nos infrastructures stratégiques et en réduisant notre dépendance à l'égard des fournisseurs de technologie non européens.

Elle se définit par notre capacité à concevoir, développer, produire, contrôler et protéger nos infrastructures numériques, englobant l'ensemble des systèmes physiques et logiciels dédiés aux centres de données, aux calculateurs haute performance, à l'informatique quantique, au *cloud*, à l'IA, aux semi-conducteurs, à la cybersécurité et aux réseaux de communication.

1. L'UE est dépendante des technologies étrangères, ce qui fait peser sur elle des risques importants.

1.1. Avec des données stockées et hébergées majoritairement en dehors de son territoire, l'UE reste fortement dépendante en matière de cloud.

Le marché européen du *cloud* est incontestablement dominé par des acteurs américains : Amazon Web Services, Microsoft Azure et Google Cloud représentent ensemble environ 69 % des parts de marché de l'infrastructure *cloud* en Europe. Les fournisseurs européens, tels qu'OVHcloud et Deutsche Telekom, ne dépassent pas les 13 %. Enfin, 92 % des données occidentales sont stockées aux États-Unis, dans des infrastructures détenues et exploitées par des fournisseurs américains.

Cette concentration pose deux problématiques :

- La dépendance infrastructurelle : l'UE n'est pas capable de répondre seule à ses besoins croissants.

- La vulnérabilité juridique : la loi Fisa permet aux agences de renseignement d'accéder aux données des entreprises technologiques américaines. Le *Cloud Act* permet aux autorités américaines d'accéder à des données hébergées par des entreprises

américaines, même si ces données sont physiquement stockées en dehors des États-Unis.

1.2. La faiblesse des investissements et une trop forte régulation accentuent le retard de l'UE dans le domaine de l'IA.

En 2021, l'UE ne représentait que 7 % des investissements mondiaux en IA, contre 40 % pour les États-Unis et 32 % pour la Chine. En 2023, l'Europe a investi environ 5 milliards d'euros en IA, contre 20 milliards d'euros pour les États-Unis. Le plan américain *Stargate* prévoit d'investir 500 milliards sur quatre ans.

Par ailleurs, le sommet de l'IA à Paris a montré que l'UE était perçue comme un facteur bloquant en raison de sa régulation.

1.3. Semi-conducteurs : une industrie stratégique en retard.

L'Europe manque d'usines de pointe capables de produire des semi-conducteurs avancés (<10 nm). L'Europe ne produit que 10 % des semi-conducteurs mondiaux, bien loin des 54 % fabriqués à Taïwan (principalement par TSMC) et des 16 % produits en Chine. En parallèle, en 2021, selon la Fédération syndicale IndustriALL, l'UE consommait 16 % de la production mondiale. Cette dépendance expose l'UE aux tensions géopolitiques et aux ruptures d'approvisionnement.

Le *European Chips Act* conduit à offrir des aides importantes à des entreprises étrangères pour implanter leurs unités de production en Europe. Si le continent européen est une simple base industrielle pour des technologies conçues et contrôlées ailleurs, cela ne garantira ni l'indépendance technologique ni l'acquisition du savoir-faire.

1.4. La maîtrise des infrastructures de communication est essentielle pour faciliter et protéger la circulation des données.

Les faiblesses européennes se manifestent au travers de trois segments clés :

- **Le segment terrestre** : Dans son Livre blanc du 21 février 2024, la Commission constate l'insuffisance de la couverture en fibre optique et les retards dans le déploiement des réseaux 5G autonomes.

- **Le segment sous-marin :** Les câbles représentent 95 % des communications internationales. L'Europe dispose d'un leader, Alcatel Submarine Networks (ASN), qui détient environ un tiers du marché mondial mais les ruptures qui ont eu lieu dans la mer Baltique montrent un manque de résilience.

- **Le segment spatial** : Alors que la société américaine Starlink compte déjà plus de 4 000 satellites en orbite, l'Europe est encore en phase de conception de ses constellations LEO.

Ces dépendances rendent l'UE vulnérable aux cyberattaques, sabotages et ingérences étrangères. En 2020, une entreprise sur huit a été touchée par des cyberattaques et ce chiffre ne fait qu'augmenter. En 2023, ce chiffre atteindrait, selon le rapport Hiscox, 58% en Allemagne et 53 % en France.

1.5. Informatique quantique et calcul haute performance (HPC) : l'UE dispose d'atouts incontestables.

L'UE a lancé son programme *Quantum Flagship* avec un budget de 1 milliard d'euros sur 10 ans et, en parallèle, 32 pays européens ont lancé l'initiative EuroHPC dotée d'un budget de 7 milliards d'euros. L'objectif est de faciliter l'accès des entreprises européennes aux capacités de calcul avancées.

Sur le sol européen, l'entreprise néerlandaise ASML produit des technologies de lithographie utilisées dans le calcul haute performance et des applications avancées, y compris l'informatique quantique. Elle permet à l'UE de conserver un maillon essentiel et une place stratégique dans la chaîne de production.

2. L'UE peut retrouver sa souveraineté technologique en misant sur la recherche et R&D, ainsi que l'investissement.

2.1. Au lieu des subventions publiques, il faut privilégier l'investissement privé dans la R&D et le développement des entreprises européennes.

L'UE saupoudre des milliers d'entreprises d'argent public, en multipliant les petites aides publiques. Cette dispersion des subventions sur trop de projets différents ne permet à aucun d'atteindre une véritable masse critique. Il faudrait favoriser les fusions et acquisitions stratégiques pour permettre l'émergence d'acteurs européens robustes en intégrant explicitement les fusions et acquisitions stratégiques dans le cadre des Projets Importants d'Intérêt Européen Commun (PIIEC).

Par ailleurs, ce sont les capitaux privés qui ont permis aux États-Unis et à l'Asie de dominer le secteur des semi-conducteurs. Les fonds de pension européens représentent 3000 milliards d'euros d'actifs mais, selon la BCE, ils n'allouent que 0,02 % de leurs actifs au capital-risque, contre près de 2 % pour les fonds de pension américains.

Recommandation n°1 : Il faudrait encourager les investisseurs institutionnels privés à investir dans un portefeuille diversifié d'entreprises technologiques européennes à fort potentiel en simplifiant le cadre réglementaire du Fonds Européen d'Investissement à Long Terme (ELTIF 2.0), en favorisant les fusions et acquisitions et en proposant, lorsque l'UE est compétente, des incitations fiscales.

2.2. Faire de la commande publique l'outil de développement de la souveraineté technologique européenne en réservant une part des marchés publics aux entreprises européennes.

La commande publique, déjà utilisée dans des secteurs comme la défense, est un levier stratégique pour stimuler la R&D en créant un environnement concurrentiel. En Chine, la totalité des marchés publics dans les secteurs stratégiques bénéficient à des entreprises nationales. Aux États-Unis, ce chiffre atteindrait 70 %. En comparaison, dans certains États membres de l'UE, seulement 8 à 12 % des commandes publiques profiteraient à des acteurs européens.

Le *Buy American Act* et le *Small business Act* n'ont pas encore d'équivalent au sein de l'UE. C'est pour cela que le rapport Draghi recommande d'introduire un « *quota minimum explicite* » pour la production locale dans les marchés publics afin d'agir comme « *client de lancement*

» pour les nouvelles technologies.

Recommandation n°2 : Il faudrait réformer le fonctionnement des marchés publics européens pour permettre aux États membres de réserver leurs marchés stratégiques aux entreprises européennes respectant des critères de souveraineté.

Lorsqu'il s'agit de données sensibles, il faudrait introduire un critère de cybersécurité européen qui prenne en considération la souveraineté. Encore en cours de discussion, le « schéma de certification européen de cybersécuritépour les services *cloud* » (EUCS) ne prévoit pas suffisamment de garanties concernant l'hébergement des données sensibles européennes, même pour son niveau de certification le plus élevé (niveau « High »). Afin de s'assurer que l'hébergeur ne soit pas soumis à une législation extra-européenne, il faudrait que la certification EUCS s'aligne sur les garanties demandées par la certification française SecNumCloud concernant les critères « d'immunité » des données aux lois extraterritoriales et de contrôle de l'entreprise.

Recommandation n°3 : Il faudrait aligner le niveau le plus élevé (niveau « High ») de la certification EUCS sur les exigences de la certification SecNumCloud.

2.3. Réduire le recours aux financements publics en mobilisant les partenariats publics-privés.

Comme le souligne le rapport Letta, les partenariats public-privé permettent de mobiliser des investissements privés tout en limitant l'impact sur les finances publiques. Malheureusement, la Directive « Solvabilité II », sur les fonds de pension, et la directive « IORP II », sur les assurances vie, imposent des règles de prudence qui sont trop strictes vis-à-vis des secteurs stratégiques et émergents.

Recommandation n°4 : Il faudrait réformer les réglementations européennes qui rendent moins attractifs les actifs considérés comme risqués et émergents, via des exigences de capital élevées et un principe de prudence trop strict.

2.4. Un choc de simplification doit alléger les fardeaux réglementaires.

La réglementation est « un obstacle à l'investissement » pour plus de 60 % des entreprises de l'UE et 55 % des PME signalent que leurs plus grands défis sont les fardeaux réglementaires. Les récents rapports de MM. Draghi et Letta ont mis en lumière le même problème.

Recommandation n°5 : Il faudrait supprimer deux réglementations pour chaque nouvelle réglementation créée dans les secteurs stratégiques, à l'instar du décret américain « *One-In, Two-Out* ».

2.5. Le renforcement des infrastructures numériques passe par une politique énergétique durable et compétitive.

Une énergie durable et compétitive est essentielle pour favoriser les investissements dans les infrastructures numériques, très consommatrices d'énergie.

Recommandation n°6 : Il faudrait réformer le marché européen de l'électricité en mettant fin au mécanisme de l'ordre de mérite, qui aligne les prix sur les ressources les plus chères, et en rétablissant un cadre permettant au nucléaire de fournir une électricité compétitive et stable.

ANNEXE: ENTITÉS OU PERSONNES DONT LA RAPPORTEURE A REÇU DES CONTRIBUTIONS

Conformément à l'article 8 de l'annexe I du règlement intérieur, la rapporteure déclare avoir reçu des contributions des entités ou personnes suivantes pour l'élaboration du projet de rapport:

Entity and/or person
Roberto Viola, Directeur Général de la DG Connect (Commission européenne)
Service de recherche du Parlement européen (EPRS)
Jean-Paul Smets, PDG de Rapid.Space
Christian Harbulot, créateur de l'École de Guerre Économique (EGE), auteur de « *La Guerre Économique au XXIe siècle, mars 2024* »
Marc Darmon, Président du Comité Stratégique de Filière « Industrie de Sécurité »
Bruno Giorgianni, Directeur de cabinet du PDG, Directeur des affaires publiques chez Dassault
Thomas Balladur, Cofondateur et Président directeur général d'Interstis
Thomas Fauré, fondateur du réseau social sécurisé Whaller
Olivier de Maison Rouge, auteur et avocat spécialisé en intelligence économique
Marc Watin-Augouard, expert en cybersécurité
Léonidas Kalogeropoulos, dirigeant du Cabinet Médiation & Arguments et Délégué Général de l'Open Internet Projet (OIP)
Thomas Volmer, Responsable de la politique mondiale de diffusion de contenu chez Netflix et Teodora Raychinova, Responsable senior des Affaires Publiques chez Netflix
Anton'Maria Battesti, Directeur des Affaires publiques France chez Meta et Simone Gobello, Responsable des politiques publiques chez Meta

La liste ci-dessus est établie sous la responsabilité exclusive de la rapporteure.

Lorsque des personnes physiques sont identifiées dans la liste par leur nom, leur fonction ou les deux, la rapporteure déclare avoir soumis aux personnes physiques concernées l'avis du Parlement européen relatif à la protection des données nº 484 (https://www.europarl.europa.eu/data-protect/index.do), qui définit les conditions applicables au traitement de leurs données à caractère personnel et les droits liés à ce traitement.