

PARLEMENT EUROPÉEN

COMMISSION DE L'INDUSTRIE,
DE LA RECHERCHE ET DE L'ÉNERGIE



**RAPPORT DE
SARAH KNAFO**
sur la souveraineté
technologique

17 mars 2025

SOMMAIRE

EXPOSÉ DES MOTIFS	3
PROPOSITION DE RÉOLUTION DU PARLEMENT EUROPÉEN	17
ANNEXE : ENTITÉS OU PERSONNES DONT LA RAPPORTEURE A REÇU DES CONTRIBUTIONS	31

L'Union européenne 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'Union 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 pour l'action sur l'IA de Paris, qui s'est tenu 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, à développer, à produire, à contrôler et à protéger nos infrastructures numériques, c'est-à-dire 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'UNION 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'Union 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'Union 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'Union dans le domaine de l'IA.

En 2021, l'Union 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 dans l'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 pour l'action sur l'IA de Paris a montré que l'Union était perçue comme un facteur bloquant en raison de sa réglementation.

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'Union consommait 16 % de la production mondiale. Cette dépendance expose l'Union aux tensions géopolitiques et aux ruptures d'approvisionnement.

Le règlement européen sur les puces («*the 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'Union vulnérable aux cyberattaques, aux sabotages et aux 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'Union dispose d'atouts incontestables.

L'Union a lancé son programme Quantum Flagship avec un budget d'un milliard d'euros sur dix ans et, en parallèle, 32 pays européens ont lancé l'initiative EuroHPC dotée d'un budget de sept 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 («HPC») et des applications avancées, y compris l'informatique quantique. Elle permet à l'Union de rester un maillon essentiel et de conserver une place stratégique dans la chaîne de production.

2. L'UNION PEUT RETROUVER SA SOUVERAINETÉ TECHNOLOGIQUE EN MISANT SUR LA RECHERCHE ET LA R&D, AINSI QUE SUR 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'Union 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 3 000 milliards d'euros d'actifs mais, selon la Banque centrale européenne, 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'Union 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 bénéficie à des entreprises nationales. Aux États-Unis, ce chiffre atteindrait 70 %. En comparaison, dans certains États membres de l'Union, 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'Union. 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 cybersécurité pour les services *cloud*» (EUCS) ne prévoit pas suffisamment de garanties concernant l'hébergement des données sensibles européennes, même pour son niveau de certification «élevé». 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 face aux lois extraterritoriales et de contrôle de l'entreprise.

RECOMMANDATION N°3 : Il faudrait aligner le niveau «élevé» de la certification EUCS sur les exigences de la certification SecNumCloud.

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

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 «IRP 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'Union et 55 % des PME signalent que leurs plus grands défis sont les fardeaux réglementaires. Les récents rapports 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.

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

SUR LA SOUVERAINETÉ TECHNOLOGIQUE EUROPÉENNE ET LES INFRASTRUCTURES NUMÉRIQUES

Le Parlement européen,

- vu le traité sur l'Union européenne (traité UE) et, plus particulièrement, son article 4,
- vu le traité sur le fonctionnement de l'Union européenne (traité FUE), notamment ses articles 173, 179 et 190,
- vu la communication COM(2021) 118 final du 9 mars 2021 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Une boussole numérique pour 2030 : l'Europe balise la décennie numérique»,

- vu la communication COM(2025) 30 final du 29 janvier 2025 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Une boussole pour la compétitivité de 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 (règlement européen sur les puces, «the 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 SRI 2),
- vu le rapport détaillé «Foresight Cybersecurity Threats For 2030 - Update 2024» [Prévision des menaces de cybersécurité à l'horizon 2030 - mise à jour 2024] de l'Agence de l'Union européenne pour la cybersécurité (ENISA),

- vu le règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques,
- vu le règlement (UE) 2025/28 du Parlement européen et du Conseil du 19 décembre 2024 établissant des mesures destinées à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir (règlement sur la cybersolidarité),
- vu le règlement (UE) 2025/37 du Parlement européen et du Conseil du 19 décembre 2024 modifiant le règlement (UE) 2019/881 en ce qui concerne les services de sécurité gérés (règlement sur la cybersécurité),
- vu le livre blanc de la Commission européenne du 21 février 2024 intitulé «Comment maîtriser les besoins en infrastructures numériques de l'Europe?»,

- 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 Mario Draghi, «The future of European competitiveness (Part A | A competitiveness strategy for Europe)» [L'avenir de la compétitivité européenne | (Partie A | Une stratégie en faveur de la compétitivité pour l'Europe)], septembre 2024,
- vu le rapport d'Enrico Letta, «More than a Market - Speed, security, solidarity - Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens» [Bien plus qu'un marché - Rapidité,

sécurité, solidarité - Donner au marché unique les moyens d'apporter à tous les citoyens européens un avenir durable et la prospérité], avril 2024,

- vu la communication COM(2024) 260 final du 2 juillet 2024 de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «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 2025» [L'économie du téléphone portable en Europe à l'horizon 2025],
- vu le Clarifying Lawful Overseas Use of Data Act [loi visant à clarifier l'utilisation légale des données à l'étranger] («Cloud Act») américain, adopté en 2018,
- vu le Foreign Intelligence Surveillance Act [loi sur la surveillance et le renseignement étranger] (FISA) américain, adopté en 1978,

- vu le Buy American Act [loi incitant à «consommer américain»] et le Small business Act [loi sur les petites et moyennes entreprises] américains,
- vu le décret présidentiel 13771, «Reducing Regulation and Controlling Regulatory Costs» [réduire la réglementation et maîtriser les coûts réglementaires] («One-In, Two-Out») [un ajout, deux retraits], 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 (IRP 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 membres différents (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 du 20 janvier 2004 relatif au contrôle des concentrations entre entreprises,
- vu la communication (2021/C 528/02528/02) du 30 décembre 2021 de la Commission 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),
- vu le rapport du service de recherche du Parlement européen rédigé par Guillaume Ragannaud, «The EU chips act: Securing Europe's supply of semiconductors» [Le règlement européen sur les puces: garantir l'approvisionnement de l'Europe en semi-conducteurs], 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 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-Unis¹, que 69 % des parts de marché européen du cloud sont détenues par des acteurs américains², contre seulement 13 % pour les acteurs européens³, ce qui expose les données européennes à des législations extraterritoriales, notamment la loi FISA et le *Cloud Act* américain;

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>

- D.** considérant que l'Union ne représente que 7 % des investissements mondiaux en intelligence artificielle (IA), bien en dessous 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 ménages⁵, tandis que les réseaux 5G «de haute qualité» ne couvrent que 50 % du territoire de l'Union⁶;
- G.** considérant qu'en 2020, une entreprise sur huit a été touchée par des cyberattaques⁷; qu'en 2023, selon le rapport Hiscox, ce chiffre atteindrait 58 % en Allemagne et 53 % en France;

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>

- 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 et le 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;
- 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 un trop grand nombre de projets différents, l'Union ne permet à aucun d'entre eux 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'Union;
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 «élevé» du schéma européen de certification 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. demande à la Commission de faciliter le déploiement de la 5G⁸ en assouplissant les conditions de concentration d'entreprises, afin d'encourager la mutualisation des infrastructures;

⁸ Rapport «The Mobile Economy Europe 2025» [L'économie du téléphone portable en Europe à l'horizon 2025].

9. invite la Commission et les commissions compétentes du Parlement à promouvoir les partenariats public-privé 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 et les semi-conducteurs; suggère d'alléger la réglementation qui rend moins attractifs les actifs risqués en imposant des exigences de capital élevées et un principe de prudence trop strict;
11. prie la Commission et les commissions compétentes du Parlement de réviser le cadre juridique des 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, sur le modèle du décret présidentiel 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 qui permette au nucléaire de fournir une électricité compétitive et stable;
- 14.** charge sa Présidente de transmettre la présente résolution au Conseil et à la Commission.

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 :

ENTITÉ OU PERSONNE
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 « <i>La Guerre Économique au XXI^e siècle, mars 2024</i> »
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 n° 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.