

A S S E M B L É E N A T I O N A L E

1 7 ^e L É G I S L A T U R E

Compte rendu

Commission des affaires étrangères

– Table ronde, ouverte à la presse, sur les ingérences étrangères dans les processus démocratiques, avec la participation de Mme Claire Benoit, cheffe du bureau *Coordination et stratégie* du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), M. David Colon, professeur agrégé d'histoire à l'Institut d'études politiques de Paris, et M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique..... 2

Mercredi
5 février 2025
Séance de 11 heures

Compte rendu n° 32

SESSION ORDINAIRE 2024-2025

**Présidence
de Mme Laëtitia
Saint-Paul,
*Vice-présidente***



La commission auditionne, dans le cadre d'une table ronde ouverte à la presse sur les ingérences étrangères dans les processus démocratiques, Mme Claire Benoit, cheffe du bureau *Coordination et stratégie* du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum), M. David Colon, professeur agrégé d'histoire à l'Institut d'études politiques de Paris, et M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique.

La séance est ouverte à 11 h 20.

Présidence de Mme Laetitia Saint-Paul.

Mme Laetitia Saint-Paul, présidente. Notre ordre du jour appelle la tenue d'une table ronde sur les ingérences étrangères dans les processus démocratiques. Ce sujet, déjà présent lors des élections américaines de 2016 et du référendum sur le Brexit la même année, prend une ampleur croissante, voire systématique. Les récentes élections en Géorgie, Moldavie et Roumanie en octobre et novembre 2024 illustrent la prégnance des risques qui pèsent sur l'intégrité et sur la sincérité de nos processus et échéances démocratiques.

Pour nous permettre de réfléchir sur cette question cruciale, je tiens à remercier les intervenants qui, ce matin, nous permettront d'évoquer le phénomène, les enjeux qu'il recouvre et ses implications, dont il nous faut tenir compte en tant que législateur.

Mme Claire Benoit, cheffe du bureau *Coordination et stratégie* du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum). Viginum, service rattaché au secrétariat général de la défense et de la sécurité nationales (SGDSN), a pour mission de protéger notre débat public numérique contre les ingérences étrangères. L'année 2024 a été marquée, pour plusieurs raisons, par un durcissement de la menace informationnelle. En premier lieu, une compétition stratégique désinhibée persiste, utilisant des actions hybrides dont la menace informationnelle est l'essence. Ensuite, les grandes entreprises du numérique se livrent à une compétition pour dominer la sphère de l'information, avec l'intelligence artificielle (IA) au cœur de cette lutte. Enfin, l'essor de l'IA générative amplifie la menace sur nos écosystèmes informationnels.

Concernant la France, trois tendances se dégagent. Premièrement, l'impact des conflits armés régionaux dépasse les frontières des belligérants et offre un terrain propice à la menace informationnelle. Deuxièmement, les scrutins nationaux demeurent attractifs pour les acteurs de la menace. Enfin, l'intérêt pour les grands événements sportifs, comme les Jeux olympiques de Paris 2024, offre un terrain d'action favorable aux ingérences numériques étrangères.

Pour protéger notre débat public, notamment lors des élections européennes et législatives anticipées, Viginum a déployé une stratégie préventive en trois axes. Le premier a consisté à ouvrir une opération de protection du débat public numérique francophone en vue de détecter et caractériser les tentatives d'ingérence. Le deuxième a reposé sur une sensibilisation des équipes de campagne des candidats, avec la distribution d'un guide disponible en ligne. Le dernier a visé à établir une coordination avec les plateformes numériques et les acteurs interministériels impliqués dans la lutte contre la manipulation de l'information.

Viginum a également été mobilisé pour protéger les Jeux olympiques et le service analyse en profondeur les opérations d'ingérence numérique étrangère observées, notamment durant les élections.

L'ingérence numérique étrangère se manifeste sous diverses formes, notamment l'usurpation d'identités d'institutions officielles ou de médias et l'utilisation de réseaux de faux comptes pour diffuser massivement la création de faux contenus crédibles grâce à l'intelligence artificielle générative et l'exploitation d'influenceurs ou de comptes populaires pour amplifier certains récits. Notre service a pu mieux comprendre les méthodes des acteurs menaçants en analysant ces opérations. Ceux-ci connaissent bien notre démocratie, notre société et nos divisions internes. Ils suivent notre actualité et cherchent à exploiter les événements polarisants. Par exemple, ils surveillent attentivement la situation dans nos départements d'outre-mer pour attiser les tensions et manipuler l'opinion publique. Leurs modes opératoires évoluent et deviennent plus persistants, nous obligeant à développer des réponses qui vont au-delà du domaine technique et opérationnel, notamment en matière d'éducation, d'information du public et de mobilisation de la société civile.

L'année dernière, notre service a exposé cinq campagnes de manipulation de l'information en collaboration avec le ministère de l'Europe et des affaires étrangères. Nous avons publié des rapports détaillant nos investigations, notamment sur les campagnes *Portal Combat* et *Matriochka*, ainsi qu'une analyse d'une manœuvre lors de la crise en Nouvelle-Calédonie impliquant le Baku Initiative Group.

Nous avons également entrepris la création d'un réseau regroupant divers acteurs de la société civile impliqués dans la lutte contre la désinformation, y compris des entités semi-institutionnelles, médiatiques et associatives. Nous collaborons étroitement avec l'éducation nationale pour fournir des ressources pédagogiques visant à renforcer la formation aux médias et l'esprit critique.

Sur le plan international, nous maintenons un dialogue étroit avec nos partenaires européens confrontés à des menaces similaires. Nous participons activement aux travaux menés dans diverses instances internationales telles que l'Union européenne (UE), l'Organisation de coopération et de développement économiques (OCDE), le G7 et l'Organisation du traité de l'Atlantique Nord (OTAN). Nous apportons également une assistance technique à plusieurs pays membres de l'UE et candidats à l'adhésion pour renforcer leurs capacités de lutte contre les manipulations de l'information, en particulier dans la détection et la caractérisation des ingérences numériques étrangères, également connues sous le nom de *foreign information manipulation and interference* (FIMI).

M. David Colon, professeur agrégé d'histoire à l'Institut d'études politiques de Paris. L'avènement de l'ère numérique a représenté un défi sans précédent pour les régimes autoritaires, craignant la propagation des idées de liberté et d'élections libres au sein de leur population. Cette menace, perçue dès 1991, s'est intensifiée avec la domination occidentale sur l'information mondiale et la suprématie américaine dans les technologies de communication.

En réponse, ces régimes ont développé une notion de souveraineté numérique et informationnelle, se traduisant par des restrictions d'accès à Internet, la censure et le contrôle des médias d'État. Ils ont également saisi cette situation comme une opportunité pour fragiliser les démocraties libérales.

Leur stratégie, que l'on pourrait qualifier de « travail de décomposition », vise à exacerber les divisions préexistantes au sein des sociétés démocratiques. Les Russes utilisent le concept de « réalité augmentée », amplifiant certains sujets clivants dans le débat public pour accentuer les divisions.

L'objectif à long terme est d'éroder la confiance des citoyens dans leurs institutions, leurs dirigeants politiques, les médias et la légitimité du travail scientifique. Plus crucial encore, ils cherchent à brouiller la distinction fondamentale entre faits et opinions, compromettant ainsi la capacité des citoyens à agir rationnellement.

Cette confusion entre opinion et fait, savamment entretenue, fragilise la capacité des citoyens à prendre des décisions éclairées. Marc Bloch évoquait ce « *minimum de renseignements nets et sûrs sans lesquels aucune conduite rationnelle n'est possible* », tandis qu'Hannah Arendt soulignait que le sujet idéal du totalitarisme était celui incapable de distinguer le vrai du faux.

Bien que les ingérences et la désinformation ne soient pas nouvelles, l'échelle et la facilité avec lesquelles elles peuvent être menées aujourd'hui sont sans précédent. Les outils qui ont longtemps fait la force des démocraties sont désormais instrumentalisés dans le but de les fragiliser à une vitesse accélérée. Cette prise de conscience collective nous réunit aujourd'hui afin d'aborder ces défis cruciaux pour nos démocraties.

Les médias sociaux représentent un danger particulier car leur modèle économique exploite nos données et notre attention, tout en filtrant l'accès à l'information. Contrairement aux médias traditionnels, ils n'offrent pas de pluralisme externe. Tous les réseaux sociaux ont une finalité lucrative, les rendant ainsi manipulables. Dans le contexte actuel, notamment avec la guerre en Ukraine, nos adversaires stratégiques comme la Russie et la Chine exploitent ces failles. L'armée chinoise a développé le concept de « guerre cognitive algorithmique », qui se déroule dans nos esprits via les algorithmes numériques. Cette guerre utilise des dispositifs publicitaires pour cibler précisément les individus, altérant le débat public à une échelle sans précédent.

La Roumanie illustre parfaitement ce phénomène. Un rapport récent de Viginum démontre comment un candidat à l'élection présidentielle, partant avec 1 % d'intentions de vote et sans campagne traditionnelle, a atteint 23 % des suffrages uniquement grâce à une campagne sur TikTok. Ce rapport met en lumière la vulnérabilité aux algorithmes de recommandation et leur impact sur la perception des utilisateurs.

Face à cette réalité, nous devons protéger l'intégrité de nos processus électoraux et de nos espaces informationnels. Il est crucial de renforcer la capacité des citoyens à détecter et résister à la désinformation, tout en préservant notre modèle démocratique. Trop souvent, les démocraties ont réagi en limitant les libertés, renforçant la défiance et confortant le discours de régimes autoritaires. Notre approche doit se concentrer sur la mise en avant des valeurs qui nous unissent plutôt que sur ce qui nous divise.

M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique. Comme mentionné au Sénat, notre rapport, élaboré conjointement par l'Institut de la souveraineté numérique et l'Institut iDFRights de Jean-Marie Cavada, souligne l'importance cruciale de l'intelligence artificielle dans les domaines que nous abordons aujourd'hui.

L'IA est devenue le moteur. Autrefois des officines comme celles de Prigojine nécessitaient de nombreux employés et des moyens techniques importants pour leurs activités d'ingérence, mais aujourd'hui le même travail peut être réalisé pour environ 400 dollars par mois, de manière entièrement automatisée. L'expérience « Inside Countercloud » l'a démontré. Un simple script – que nous appelons *prompt* dans notre jargon – indique à l'intelligence artificielle ce qu'elle doit faire : cibler des populations spécifiques, favoriser ou handicaper des candidats, etc. L'IA envoie ensuite des millions de messages personnalisés sans intervention humaine. La personne ciblée pense qu'elle communique avec une personne réelle.

Cette démultiplication des capacités d'ingérence via l'IA est sans précédent. Contrairement aux espoirs nés lors du Printemps arabe concernant les réseaux sociaux comme outils de libération, il est possible aujourd'hui d'avoir une vision différente de l'impact sur les sociétés en question. Les courtiers en données peuvent réunir des dizaines de milliers de paramètres par individu, couvrant tous les aspects de la vie, y compris les aspects médical, philosophique, sexuel et politique.

Ces avancées permettent de manipuler les individus comme jamais auparavant, en utilisant des profils psychologiques extrêmement précis, plus détaillés que ce que pourraient connaître les proches d'une personne. Des études ont démontré la capacité de dresser des profils psychologiques, politiques et sexuels bien plus précisément qu'avec des méthodes traditionnelles.

Je souhaite revenir sur la vulnérabilité considérable de l'Europe dans le domaine du numérique, qui s'explique par notre manque d'industrie dans ce secteur. Je citerai un propos de Barack Obama en 2015, qui illustrent bien la perception américaine : « *Lorsque les Européens s'interrogent sur les notions de données personnelles et de protection des libertés, ce n'est qu'une façon hypocrite d'essayer de mettre en avant leurs intérêts commerciaux et de nous ralentir, nous, Américains qui avons fondé l'Internet et qui l'avons développé* ».

Cette attitude persiste. Lors des négociations aux Nations unies sur la gouvernance de l'Internet, nos interlocuteurs américains nous accusaient de geindre parce que nous n'avions pas d'industrie. Tant que nous n'aurons pas d'industrie comparable aux géants comme TikTok ou X, nous resterons vulnérables. Toute loi sera contournable et contournée.

Une nouveauté émerge : la défense des droits humains, de l'intégrité des élections et la lutte contre les ingérences étrangères passent désormais par une politique industrielle. Ces notions, autrefois découplées, sont aujourd'hui intimement liées.

Il est frappant de voir comment nos adversaires utilisent nos instruments démocratiques contre nous. Par exemple, TikTok invoque la liberté d'expression aux États-Unis, alors que son équivalent en Chine est sévèrement censuré. L'Inde a totalement banni TikTok et l'idée d'interdire certaines plateformes, comme nous l'avons fait pour Russia Today et Sputnik au début de la guerre en Ukraine, n'a plus rien d'anormal.

Les services de renseignement américains s'inquiètent à juste titre de la capacité d'espionnage de TikTok. J'ai déjà déclaré que pour les services chinois, ne pas utiliser ces données à des fins d'espionnage serait une faute professionnelle.

Notre équilibre démocratique nécessite un réinvestissement massif, comme le propose le rapport de Mario Draghi avec 800 milliards d'euros par an, soit 5 % du produit

intérieur brut européen (PIB). Sans grand financement, l'Europe risque de devenir une citadelle assiégée par trois empires : la Chine, la Russie et les États-Unis.

Il faut abandonner notre naïveté passée et comprendre que le salut passe aussi par une réponse industrielle et stratégique. Vous, législateurs, serez les premiers acteurs de cette prise de conscience, tant au niveau français qu'europpéen. Sans elle, comme le souligne le rapport de Mario Draghi, il pourrait être question dans les années à venir de l'agonie européenne.

Mme Laetitia Saint-Paul, présidente. Les orateurs des groupes politiques vont à présent s'exprimer.

M. Julien Gokel (SOC). Les tentatives d'ingérences étrangères dans nos processus démocratiques s'inscrivent dans le temps long, manipulant l'opinion publique, accentuant nos divisions, polarisant les débats et affaiblissant la confiance dans nos institutions. Ces ingérences prennent des formes diverses, allant des cyberattaques aux influences sur les réseaux sociaux, en passant par l'instrumentalisation des diasporas et le soutien d'acteurs politiques ou médiatiques favorables aux intérêts étrangers.

Face à ces menaces, nos institutions ont réagi, notamment avec la loi de juillet 2024 visant à prévenir les ingérences étrangères et la création de commissions d'enquête au niveau national et européen. Mais ces mesures sont-elles suffisantes ? Notre arsenal juridique est-il adapté ? Avons-nous les moyens nécessaires pour surveiller, détecter et contrer efficacement ces ingérences, particulièrement les campagnes de désinformation sur les plateformes étrangères ?

La souveraineté numérique de la France et de l'Europe est souvent évoquée comme un rempart possible. Comment pouvons-nous réduire notre dépendance aux grandes plateformes étrangères ? Ces dernières coopèrent-elles ou constatez-vous un recul, comme avec Meta qui a mis fin à ses partenariats de *fact-checking* ?

L'Union européenne s'est dotée des règlements DMA (*Digital markets Act*) et DSA (*Digital services Act*) pour encadrer les marchés et services numériques. Cependant, leur application insuffisante ne permet pas de contenir efficacement les ingérences. La Roumanie est devenue le premier État membre à voir ses élections invalidées en raison d'une ingérence massive de désinformation sur TikTok.

Au groupe socialiste, nous estimons que ces règlements doivent être appliqués pleinement et efficacement. Pourquoi ne le sont-ils pas ? L'Union doit être plus ambitieuse dans ce domaine. Enfin, nous appelons à une stratégie européenne de développement de plateformes et d'infrastructures souveraines. Sans cela, nous resterons dépendants de multinationales qui ne partagent pas toujours nos valeurs démocratiques.

Mme Claire Benoit. La création de Viginum, il y a trois ans et demi, témoigne de la volonté et de la prise de conscience de l'État face au phénomène des manipulations de l'information. La France est à l'avant-garde en Europe, et au-delà, dans le déploiement de moyens pour faire face à cette menace. Nous disposons d'un cadre juridique clair et strict, notamment en matière de collecte automatisée de données à caractère personnel, ce qui constitue une protection pour nos citoyens et notre démocratie. Viginum travaille uniquement en sources ouvertes, sans être un service de renseignement ou de police. Nous collaborons avec l'ensemble des acteurs étatiques disposant de moyens pour lutter contre les

manipulations de l'information, couvrant tout le spectre du traitement de ces menaces, de la veille à la réponse.

Concernant le DSA, Viginum a signé une convention avec l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) en juillet 2024. Nous apportons notre expertise technique sur le fonctionnement des plateformes, notamment sur la manière dont leurs fonctionnalités peuvent être détournées à des fins malveillantes ou d'ingérence. Nous collaborons étroitement avec l'Arcom dans le cadre des enquêtes ouvertes par la Commission européenne contre plusieurs plateformes. Nous documentons tout potentiel manquement à leurs obligations au titre du DSA, en particulier concernant l'accès aux API (*Application programming interfaces*) et aux régies publicitaires.

M. Bernard Benhamou. Je partage les interrogations soulevées sur la souveraineté. Cette notion, issue de nos travaux aux Nations unies en 2006, était considérée comme de la science-fiction lors de la création de l'Institut en 2015. Aujourd'hui, elle est omniprésente dans les discours.

Le véritable enjeu réside dans sa définition et sa mise en œuvre par la puissance publique, sachant que l'Europe est loin d'être exemplaire en la matière. Notre dépendance technologique est considérable, avec 80 % de nos achats technologiques effectués hors Europe, comme le soulignent les rapports de Mario Draghi et d'Enrico Letta. La réduction de notre surface d'attaque nécessite un rééquilibrage et la fin de la naïveté de l'action européenne dans ce domaine. Ce choix stratégique est un muscle politique à déployer, crucial dans la période à venir.

Mme Clémentine Autain (EcoS). J'ai été intéressée par le propos de David Colon sur le paradoxe du régime chinois mais je suis étonnée que l'on n'aborde pas davantage la nouveauté du moment : l'offensive au sein même des régimes prétendus démocratiques. L'exemple d'Elon Musk, avec son salut fasciste et ses propos, ainsi que celui de Zuckerberg et leur rapport au régime trumpien illustrent ce phénomène. Leur discours prônant une liberté totale de circulation de l'information masque en réalité le contrôle exercé par quelques milliardaires sur les algorithmes et nos données.

Cette situation soulève des questions sur nos relations internationales et notre vision des sociétés dites « démocratiques ». L'utilisation du mot « liberté » par des figures comme Javier Milei dans son discours au Forum de Davos est particulièrement frappante car elle sert à justifier la remise en cause de libertés fondamentales.

Je souhaiterais également insister sur l'importance de notre politique industrielle, comme l'a mentionné Bernard Benhamou. L'État français s'est longtemps dépossédé de sa capacité d'action dans ce domaine. Comment pouvons-nous avoir un acteur public qui entre dans le jeu, notamment en termes de réglementation ? Des entreprises publiques comme France Télécom ou La Poste ne se sont pas intéressées à la révolution numérique, malgré la présence d'ingénieurs de haut niveau. Que pouvons-nous faire pour remédier à cette situation ?

M. David Colon. Concernant Elon Musk, il est important de noter qu'il a interféré dans plusieurs processus démocratiques en remettant en cause les gouvernements canadien, irlandais, britannique et allemand. Cependant, il n'a pas critiqué les gouvernements chinois ou russe. Sa liberté d'expression semble limitée par ses intérêts économiques, notamment les investissements réalisés par des proches de Vladimir Poutine dans le rachat de Twitter ou ses

relations industrielles en Chine. De fait, son action peut le faire apparaître comme un agent d'influence du Kremlin et de la Chine, relayant leurs discours, en correspondance avec leurs attentes.

Cette situation illustre un point crucial, nous nous concentrons sur les ingérences étrangères mais il faut également considérer les manipulations de l'information au sein même de nos espaces démocratiques. Les régimes autoritaires cherchent des agents d'influence, qu'ils soient rémunérés, traités par leurs services de renseignement ou agissant par conviction personnelle, idéologique ou par ignorance, pour relayer leurs discours et leurs attentes.

Mon analyse révèle que, sur le long terme, les régimes autoritaires ont cherché à fragiliser certains fondements des États-Unis en trouvant des alliés objectifs, notamment dans le mouvement soutenant le président Trump et chez certains techno-oligarques comme Elon Musk. Concernant la liberté d'expression, depuis que ce dernier a pris le contrôle de Twitter, rebaptisé X, le nombre de suppressions de comptes n'a jamais été aussi élevé. De plus, il a demandé à quatre-vingts ingénieurs de modifier les algorithmes de recommandation pour que son propre compte apparaisse sur tous les profils, qu'on soit abonné ou non, et pour attribuer à chacun de ses tweets un multiplicateur de puissance par mille. Cette approche rend quasi impossible d'échapper à ses publications, ce qui représente une conception pour le moins étrange de la liberté d'expression.

Mme Maud Petit (Dem). Les ingérences ont toujours existé mais, aujourd'hui, elles proviennent principalement de Russie, de Chine, de Turquie et d'Iran et sont facilitées par les outils numériques. En tant qu'élue du Val-de-Marne d'origine martiniquaise, je m'inquiète des tentatives d'influence et de déstabilisation organisées contre l'intégrité territoriale de la France par l'Azerbaïdjan, notamment dans les territoires d'outre-mer. L'Azerbaïdjan soutient ouvertement les mouvements indépendantistes ultramarins à travers le Baku Initiative Group (BIG).

Ce groupe a récemment réuni à Bakou des mouvements indépendantistes des territoires d'outre-mer et de Corse, actant la création d'un front international de libération des colonies françaises. Le BIG est également très actif sur les réseaux sociaux. En décembre 2024, Viginum a épinglé ses campagnes de désinformation menées contre la France. Le ministre des outre-mer a fermement condamné ces opérations d'ingérence. Le Parlement a adopté une loi en juillet 2024 pour renforcer les dispositifs de prévention et d'entrave aux ingérences. Au-delà des condamnations et de la loi, de quels leviers dispose notre pays pour lutter efficacement contre ces ingérences ?

Mme Claire Benoit. L'Azerbaïdjan fait effectivement partie des compétiteurs qui n'étaient pas initialement dans notre radar. Notre rôle est d'observer et de mettre en lumière l'implication d'acteurs étrangers dans des campagnes numériques ciblant nos intérêts. L'imputation technique et l'attribution politique relèvent respectivement des services de renseignement et des décideurs politiques.

Concernant le BIG, nous l'avons détecté dès juillet 2023, dans le cadre d'une campagne appelant au boycott des Jeux olympiques. Nous avons observé des comptes pro-azerbaïdjanais ciblant les intérêts français dans ce contexte. Cette campagne a fait l'objet d'un rapport non public. Le BIG se présente comme une organisation non gouvernementale (ONG) défendant les mouvements anticoloniaux et s'est rapproché des indépendantistes dans nos départements et régions d'outre-mer (DROM) et collectivités d'outre-mer (COM) avec une intention d'amplifier ses actions dans le champ informationnel.

M. Laurent Mazaury (LIOT). Vos propos sont inquiétants, bien que nous en ayons déjà conscience. Je rappelle que la position de l'Azerbaïdjan est similaire dans le dossier arménien, où la France est impliquée.

Dans un monde de plus en plus interconnecté, nous constatons une montée des ingérences étrangères dans nos processus démocratiques, notamment *via* les réseaux sociaux. Comment évaluez-vous l'impact de ces ingérences sur les élections et le processus démocratique en France ? Quelles mesures concrètes peut-on mettre en place pour protéger l'intégrité de notre démocratie face à ces menaces, tout en préservant la liberté d'expression et la transparence sur les plateformes numériques ? Pourquoi ne peut-on pas reproduire immédiatement le contrôle que nous exerçons déjà sur nos médias télévisuels *via* l'Arcom, y compris pour les plus petites télévisions et les campagnes électorales locales, en appliquant une égalité de traitement, sur ces nouveaux médias numériques ?

M. Bernard Benhamou. Au sujet du degré d'ingérence en France, il est déjà important. On peut remonter aux *MacronLeaks* de 2016 et, à chaque époque, ont existé des tentatives similaires. Aux États-Unis, l'affaire *Cambridge Analytica* a été documentée comme étant liée aux services russes, malgré certaines tentatives de le nier. Concernant les réseaux sociaux, Facebook supprime en moyenne entre 800 millions et 1 milliard de faux comptes par trimestre, avec des pics allant jusqu'à 2 milliards.

La France est particulièrement ciblée car nous sommes considérés comme la « tête de gondole » européenne dans ces domaines. Le modèle économique des plateformes numériques a intégré la radicalisation et la polarisation comme éléments clés. Des études sociologiques ont montré que plus une vidéo est politiquement radicale, plus elle génère de vues et de partages, créant ainsi de « l'engagement ».

Si nous ne développons pas d'autres types de services avec des modèles économiques différents, cette situation risque de se reproduire indéfiniment. En tant que patrie de la Déclaration des droits de l'Homme, nous sommes particulièrement exposés. Pour la première fois, nous sommes au point de convergence de trois empires ayant intérêt à déstabiliser les démocraties.

Tant que nous ne modifierons pas notre attitude, nous resterons vulnérables. J'insiste sur l'importance de la politique industrielle, un concept souvent considéré comme dépassé. Nous sommes face à des plateformes continentales chinoises et américaines qui pratiquent un protectionnisme à tous les niveaux, à l'image de l'*Inflation Reduction Act* aux États-Unis.

Nous devons employer les mêmes armes qu'on utilise contre nous, non pas pour stopper les échanges mais pour rééquilibrer la situation et prendre en compte les risques politiques. Comme le dit Kate Crawford dans son ouvrage *Contre-atlas de l'intelligence artificielle*, « *l'IA est aujourd'hui la politique par d'autres moyens* », reprenant ainsi les mots de Clausewitz.

M. Guillaume Bigot (RN). Les ingérences étrangères dans nos institutions se multiplient de manière préoccupante, mettant en question l'intégrité de nos procédures démocratiques. Cependant, il semble que certaines ingérences soient considérées comme plus problématiques que d'autres, notamment celles venant de Moscou ou de l'administration Trump.

Bien qu'aucune ingérence ne soit acceptable, pourquoi certaines ne suscitent-elles ni débat ni indignation ? Par exemple, lorsque le recteur de la Grande Mosquée de Paris critique Boualem Sansal, ses mots ne choquent personne. Quand le groupe de Bakou, financé par Moscou, soutient les prétentions des Comores sur Mayotte, nous protestons à juste titre. Mais lorsque François Fillon révèle que Washington avait mis sur écoute son téléphone et celui du président de la République, l'indignation est moindre.

Il semble y avoir une distinction entre « bonne » et « mauvaise » ingérence. L'appel de Barack Obama à voter pour Emmanuel Macron est perçu comme une bonne ingérence, tandis que la prise de position d'Elon Musk sur un scrutin européen est vue comme une mauvaise ingérence.

D'autres formes d'ingérences, plus subtiles et souvent légales, sont tout aussi préoccupantes. Par exemple, Nathalie Loiseau, à la tête de l'organe anti-ingérences du Parlement européen, siège au European Council on Foreign Relations, financé par George Soros.

Bruxelles est devenue un centre d'influence majeur, avec trente mille lobbyistes officiellement inscrits, soit quarante-deux par parlementaire européen. La Commission européenne a même financé des ONG à hauteur de 5 milliards d'euros pour influencer son propre texte sur le *Green Deal*, une situation qui soulève des questions sur la séparation des pouvoirs.

Ma question est la suivante : ne pensez-vous pas que l'ingérence grossière de pays hostiles est plus facile à contrer que cette ingérence plus insidieuse et massive ? Et comment protéger nos institutions contre des influences, voire des ingérences, parfois institutionnalisées ?

M. David Colon. Le Parlement français a apporté une réponse à travers la loi du 25 juillet 2024 sur les ingérences étrangères. Cette loi repose sur le principe de transparence, permettant de traiter toutes les ingérences sur un pied d'égalité, qu'elles soient menées pour le compte d'un agent étranger étatique ou non. Bien que la loi soit entrée en vigueur, je m'interroge sur les moyens accordés à la Haute Autorité pour la transparence de la vie publique (HATVP) pour tenir à jour le registre, ainsi qu'à nos services d'enquête pour identifier les acteurs qui se soustrairaient à cette obligation. La transparence totale sur les ingérences est cruciale pour les évaluer justement.

Concernant la hiérarchie des menaces, le Kremlin est actuellement considéré comme la menace prioritaire en raison de l'intensité et des effets de ses ingérences, menant une guerre de l'information systématique contre les pays soutenant l'Ukraine. Plus notre soutien sera ferme, plus nous serons confrontés à des opérations de guerre hybride d'un nouveau genre.

Notre responsabilité collective est de nous doter d'outils permettant une transparence totale sur ces ingérences. Viginum contribue à la détection et à la caractérisation de ces menaces, tandis que le SGDSN participe à leur recherche et, si nécessaire, à leur imputation politique, mettant en lumière ce qui était auparavant obscur.

Mme Claire Benoit. Notre service est chargé de caractériser les ingérences numériques étrangères. Nous adoptons une approche agnostique concernant les acteurs étrangers, surveillant les écosystèmes numériques et informationnels. Dès que nous détectons l'utilisation de moyens inauthentiques, artificiels ou automatisés pour interférer dans le débat

public numérique lié aux intérêts fondamentaux de la nation, nous les identifions, les documentons et, dans certains cas, les dénonçons publiquement.

Je vous invite à consulter notre rapport public sur les manœuvres informationnelles ciblant les Jeux olympiques et paralympiques de Paris. Vous constaterez que divers écosystèmes, pas uniquement ceux des pays fréquemment cités, ont visé cet événement majeur.

M. Vincent Ledoux (EPR). Vos propos, à la fois passionnants et angoissants, évoquent un vocabulaire guerrier. La guerre, comme l'a dit Clausewitz, est la continuation de la politique. Cependant, il est devenu difficile de faire de la politique lors des derniers scrutins électoraux car nous sommes confrontés à des citoyens qui n'ont parfois qu'une seule source d'information : les médias sociaux, voire uniquement TikTok.

Dans la guerre, on distingue trois aspects : l'armée avec ses chefs, le gouvernement avec ses leaders et le peuple. Je souhaite interroger Madame Benoît sur l'apprentissage et la pédagogie nécessaires, particulièrement pour la jeunesse qui façonnera l'avenir.

Deuxièmement, en tant qu'historien, je constate que nous sommes en paix depuis longtemps, ayant peut-être entraîné un certain relâchement. Nous vivons dans un monde relativiste où tout semble se valoir, où la distinction entre faits et opinions devient floue. Ne nous sommes-nous pas trop ramollis ? Ne faut-il pas, en plus du développement industriel, un réarmement moral, une forme de sursaut ? Nous sommes visiblement très attaqués dans une guerre asymétrique, qui ne dit pas son nom et se présente souvent sous une forme séduisante. Nos ancêtres étaient constamment dans l'idée de la guerre. Aujourd'hui, le relativisme et une certaine forme d'assoupissement ne nous rendent-ils pas moins vigilants à la menace réelle qui attaque à nos fondements les plus profonds ?

Mme Claire Benoît. Votre question me permet de détailler davantage nos démarches et initiatives, notamment avec l'éducation nationale. Face à la persistance de cette menace et à l'évolution des usages des réseaux sociaux, il nous est apparu indispensable de participer à la sensibilisation et à la mobilisation des citoyens eux-mêmes.

Nous publions des rapports objectifs et documentés pour faire prendre conscience de la réalité qui pèse sur nos démocraties. Nous travaillons conjointement avec l'éducation nationale à la conception et à la production de ressources éducatives. Depuis deux semaines, une fiche pédagogique sur la lutte contre les manipulations de l'information est disponible sur Educ'ARTE, permettant aux enseignants d'aborder ce sujet en classe.

Nous avons l'ambition de créer une académie à l'horizon 2025-2026 dans le but d'organiser et de développer nos initiatives de sensibilisation. Nous visons non seulement les jeunes publics, prioritaires en tant que futurs citoyens, mais aussi d'autres publics cibles comme les entreprises, le secteur économique et les élus. Notre objectif est d'intervenir auprès des collectivités territoriales et de tous les publics que nous estimons intéressés par une sensibilisation à cette menace en vue d'accroître leur connaissance et leur vigilance.

M. David Colon. Nous sommes confrontés à une guerre psychologique et cognitive menée contre l'esprit de nos concitoyens *via* les algorithmes. Je préconise l'adoption d'une stratégie nationale de défense psychologique, comme je l'ai proposé dans la revue *Défense nationale*. L'objectif n'est pas de créer un ministère de la vérité mais de renforcer la résilience psychologique de nos concitoyens face aux manipulations de l'information. Cela passe par

des tests évaluant leur sensibilité aux récits des informateurs, des campagnes d'information sur les stratégies de nos compétiteurs dans le domaine informationnel et des campagnes de pré-bunking expliquant les techniques de manipulation utilisées en vue de fragiliser le débat public. Des solutions existent, notamment grâce à l'IA générative. Cette bataille pour les esprits n'est pas perdue mais elle est cruciale.

Mme Nathalie Oziol (LFI-NFP). Au nom du groupe La France insoumise, je souhaite souligner que si les dangers des ingérences russe, chinoise et iranienne sont réels, nous ne devons pas occulter l'ingérence assumée des États-Unis, notamment *via* les réseaux sociaux. Notre diplomatie insoumise plaide pour le non-alignement, contrairement à l'atlantisme prôné par Donald Trump. Nous estimons que ce non-alignement doit s'étendre au domaine numérique.

Elon Musk, *via* la manipulation des algorithmes de X (ex-Twitter), a contribué à la victoire de Trump et se livre à des opérations de déstabilisation politique en Europe. Au Royaume-Uni, il a soutenu des figures d'extrême droite comme Nigel Farage et Tommy Robinson, s'attaquant directement au premier ministre et à des membres du gouvernement. En Allemagne, il a apporté son soutien au mouvement d'extrême droite Alternative für Deutschland (AfD).

Ces interventions, bien que parfois traitées comme anecdotiques, sont inquiétantes compte tenu de l'importance du numérique dans l'organisation politique et sociale. La France n'est probablement pas épargnée par ces ingérences. L'espace numérique est devenu aussi important politiquement que l'espace géographique physique. Comment intégrez-vous cette forme particulière et agressive d'ingérence dans vos travaux et réflexions, étant donné l'importance cruciale de ces plateformes dans le débat public et la diffusion de l'information ?

Mme Claire Benoit. Notre approche est totalement agnostique. Nous surveillons divers écosystèmes numériques étrangers, y compris les stratégies des mouvances nationales identitaires de l'*alt-right* anglo-saxonne, bien structurées dans le champ informationnel. Notre objectif est de détecter toute tentative d'interférence dans notre débat public numérique français. Nous ne travaillons pas directement sur les débats publics ou les élections d'autres pays mais nous collaborons sur les modes opératoires pour anticiper et prévenir leur réplication dans nos propres élections.

Concernant Elon Musk et X, la question de savoir s'il s'agit d'un hébergeur ou d'un éditeur d'opinion ou d'information est une question juridique non tranchée sur laquelle je ne peux pas me prononcer.

M. Bernard Benhamou. Elon Musk peut être considéré comme un Bannon 3.0, avec des moyens colossaux. On assiste à l'émergence d'un nouvel acronyme inquiétant, MEGA (*Make Europe great again*), qui fait de l'Europe une cible explicite.

Le débat sur la responsabilité des plateformes concernant leur contenu aurait dû être tranché il y a dix ans. Initialement, l'idée était de ne pas étouffer les sociétés émergentes mais le danger s'est matérialisé récemment.

Le véritable problème aujourd'hui n'est pas seulement la responsabilité des contenus mais l'amplification. Sur des plateformes comme TikTok, un message peut être amplifié auprès de dizaines de millions de personnes, parfois à l'insu de son auteur. L'opacité algorithmique est au cœur du problème.

Je vous recommande la lecture du livre de Frank Pasquale *Black Box Society* sur la société boîte noire, qui plaide pour une transparence démocratique des algorithmes. Au-delà de la responsabilité des plateformes telle que définie dans le DSA et le DMA, l'enjeu juridique majeur est d'obtenir un accès démocratique à ces algorithmes pour comprendre comment ils amplifient certains contenus. Le projet américain concernant TikTok visait à avoir accès à la plateforme pour comprendre le fonctionnement de l'algorithme.

Mme Laetitia Saint-Paul, présidente. Je m'exprimerai également au nom de mon groupe Horizons & indépendants. Nous avons constaté que nos démocraties étaient fragiles et il est de notre responsabilité de donner à l'État les moyens de contrecarrer les velléités malveillantes qui se propagent. À ce titre, nous apportons notre pierre à l'édifice au sein de la commission, puisque mon collègue Alain David et moi-même avons été désignés pour mener une mission d'information portant sur l'irruption de l'intelligence artificielle dans les ingérences étrangères.

À ce titre, je m'interroge sur la superposition des ingérences non étatiques, celles à caractère terroriste ou criminel. Nous avons en effet vu que le narcotrafic avait pu déstabiliser des pays européens. La rétorsion étant actuellement défensive, quelles sont des mesures offensives que nous pourrions mettre en œuvre ?

Mme Claire Benoit. Notre approche est pondérée puisque l'IA, aujourd'hui, est un outil de menace ; en tout cas, elle permet de décupler la capacité à générer du contenu sans toutefois pouvoir encore accélérer les processus de diffusion. La clé dans l'amplification est bien la diffusion. L'IA permet de générer des contenus de manière massive mais ne permet pas de multiplier les canaux de diffusion. En contrepoint, nous utilisons évidemment l'IA en tant qu'outil positif puisque nous la mettons au service de la détection et de la caractérisation des ingérences numériques étrangères. Cette technologie facilite aussi le travail de nos analystes. Nous avons en notre sein une équipe, un *data lab* composé de *data scientists*, qui exploite tous les aspects positifs de l'IA dans le but d'aider le travail au quotidien de nos analystes.

Concernant la possibilité de recourir à des méthodes plus offensives, je ne m'exprimerai pas dessus puisque nous sommes un bouclier. Viginum est au cœur de la protection et du champ défensif car la lutte contre la manipulation de l'information est par essence défensive. Cette mission revient d'ailleurs au premier ministre. Néanmoins, je formulerai une petite remarque : les acteurs malveillants qui nous ciblent cherchent aussi à nous faire déraiser. Finalement, en insistant et en nous saturant au quotidien, ils cherchent à nous faire prendre des mesures attentatoires à nos libertés.

L'équilibre est fragile, il faut le garder en tête.

M. Bernard Benhamou. Il est nécessaire de développer des mesures offensives. Je citais l'interdiction des chaînes de télévision russes paneuropéenne : pour beaucoup de Français, cette décision était purement locale alors qu'elle s'avérait paneuropéenne. Nous devons effectivement arbitrer entre le risque d'attenter brièvement, temporairement, à une certaine forme de liberté d'expression et le risque démocratique, en vue de s'interroger, en particulier sur TikTok.

Toutes les plateformes sont instrumentalisées par des forces étrangères ou des forces hostiles, pas forcément étatiques ; néanmoins TikTok, du fait de sa masse, de son instrumentalisation par le régime chinois, pose un problème particulier. Malgré l'opacité, les

intérêts sont bien compris. TikTok est un merveilleux outil pour les Russes, on l'a vu en Roumanie mais pas seulement. Il est très difficile de trouver des vidéos antirusses, évidemment antichinoises, sur la plateforme.

Effectivement, nous devons nous interroger sur des mesures plus dures. Je ne prononcerai pas sur les attaques cyber qui ne relèvent pas effectivement du même registre mais, d'un point de vue législatif, nous devons nous en préoccuper.

Mme Christine Engrand (NI). Aujourd'hui, dans l'état des finances de la France, pensez-vous que nous pourrions envisager de participer à la lutte contre ces ingérences ? Quand vous parlez de réindustrialisation, avez-vous des éléments à nous confier ?

M. Bernard Benhamou. Ces éléments figurent parmi les recommandations de notre rapport.

L'état actuel des finances de l'ensemble des pays européens, pas uniquement de la France, a été impacté par la double crise, à la fois du Covid et de la guerre en Ukraine. Est-ce qu'il nous faut considérer comme stratégique et vital l'action des deux anciens premiers ministres italiens Letta et Draghi ? Cet investissement serait de « la bonne dette » pour l'Europe.

L'économiste italo-américaine Mariana Mazzucato dit qu'il n'existe pas une seule technologie clé de l'iPhone qui n'ait été financée sur des fonds fédéraux, en particulier militaires américains. Pensons au GPS (*Global Positioning System*), à l'Internet créé par la Defense advanced research projects agency (DARPA). Toutes les technologies d'intelligence artificielle, de reconnaissance de formes, de réalité augmentée ou virtuelle ont d'abord été développées sous un prisme militaire. Si nous n'articulons pas mieux la recherche civile et la recherche militaire au travers d'un abondement européen dans ces domaines, les mêmes causes produiront les mêmes effets. Nous serions, pour reprendre l'article du *Monde* paru sous peu, contraints à rester dans une trappe à médiocrité technologique.

Créer un endettement à hauteur de 5 % du PIB européen est donc bien justifié.

Mme Laetitia Saint-Paul, présidente. Nous en venons maintenant aux questions et interventions des collègues souhaitant s'exprimer à titre individuel.

Mme Pascale Got (SOC). Raphaël Glucksmann a expliqué que, si nous déplorions un nombre élevé d'attaques contre notre pays, Taïwan en subissait quotidiennement. Les autorités ont fait le choix d'y répondre par la démocratie en mettant au point de très intéressants processus démocratiques et de coopération avec la société civile. L'eurodéputé qualifiait la démocratie numérique développée dans ce pays de très impressionnante et soulignait que la lutte menée contre les campagnes de manipulation de l'information avait été beaucoup plus efficace que de toutes les actions conduites jusqu'à présent à l'échelle européenne ou française. Avez-vous des éléments pour nous éclairer sur ce qui a été mis en place dans ce pays ?

M. David Colon. En 2018, les citoyens taïwanais ont pris conscience des interférences massives provenant de Chine continentale. Depuis, la société civile s'est mobilisée pour protéger l'espace public des ingérences du parti communiste chinois. L'Organisation de coopération et de développement économiques a mis en avant l'approche transversale de Taïwan, unissant des acteurs qui ne collaborent habituellement pas sur ces

questions. Cette approche s'est concrétisée par la création d'ONG en ligne mettant en place des outils d'information. Taïwan est considéré comme un modèle vertueux en matière de lutte contre les manipulations de l'information, étant une jeune démocratie ayant su s'enraciner et contrer les ingérences chinoises. D'autres exemples existent, comme la Moldavie, la Finlande et l'Ukraine, qui ont démontré la capacité de leur société civile à se mobiliser.

En France, nous pouvons attendre beaucoup de notre société civile et des entreprises pour contribuer à la protection de la démocratie. Une proposition non retenue des États généraux de l'information était d'étendre le champ de la responsabilité sociétale des entreprises (RSE) à la protection de la démocratie, incluant par exemple le non-financement de la désinformation par des campagnes publicitaires à l'aveugle et le soutien aux actions renforçant l'esprit critique à l'école. Sans la mobilisation de la société civile, il est difficile de faire face efficacement à des déstabilisations de cette ampleur.

Mme Claire Benoit. Nous observons attentivement les pratiques de nos partenaires étrangers, notamment le modèle taïwanais en termes de partenariat avec la société civile. Nous avons déjà entrepris des collaborations avec l'éducation nationale, les médias et les grands groupes médiatiques pour partager les bonnes pratiques, notamment en matière d'*open source intelligence* (OSINT). Nous travaillons également avec des universités ayant des laboratoires spécialisés dans les problématiques de manipulation de l'information. Notre objectif est de créer un réseau fédérateur de l'écosystème impliqué dans la protection de notre démocratie. Cette ambition se reflétera dans la future académie que nous souhaitons mettre en place dans les mois et années à venir.

M. Jérôme Buisson (RN). Ma question porte sur la multiplication des pays capables d'ingérences dans le futur, du fait du partage de la technologie et de l'*open source*. La multiplication des ingérences ne les rend-elle pas moins opérantes, les unes annulant ou réduisant la capacité des autres, notamment lors d'élections où différents pays pourraient interférer dans des sens opposés ?

M. Bernard Benhamou. Malheureusement, à l'heure actuelle, ces ingérences vont toutes dans le même sens : la remise en cause des démocraties. Par exemple, lors des campagnes menées par l'Internet research agency aux États-Unis, les ingérences relevées visaient à la fois la communauté afro-américaine et les communautés évangélistes, cherchant à stimuler le vote trumpiste tout en désactivant le vote démocrate.

L'idée que ces campagnes pourraient s'auto-annihiler est peu probable car elles convergent vers le même objectif. Le vrai danger aujourd'hui n'est pas tant que les gens croient à des choses fausses qu'ils ne croient plus aux choses vraies. Les *deepfakes* et autres technologies nous mithridatisent face à la vérité, ce qui est extrêmement dangereux.

M. David Colon. Notre société peut effectivement développer une immunité collective face à une avalanche d'ingérences. L'« effet Viginum », par exemple, illustre l'impact des dénonciations successives des campagnes d'interférences russes sur le traitement médiatique de ces opérations. On a pu observer une évolution dans la réaction des médias, passant d'un battage médiatique intense à une forme d'immunisation. L'objectif est de favoriser une absence de réaction, comme on peut l'observer en Finlande, où les ingérences quotidiennes ont très peu d'impact sur le débat public.

M. Frédéric Petit (Dem). En tant que député des Français installés en Europe centrale, en Allemagne et dans les Balkans, je souhaite aborder la construction de la guerre

hybride russe dans les années 2000. Elle part du postulat que la guerre froide avait été gagnée par une guerre hybride inversée. La Russie nous accuse d'ingérence et nos efforts pour travailler avec la société civile sont souvent perçus comme une intrusion. Comment intégrez-vous cette problématique dans vos réflexions, sachant que plus on essaie de répondre, plus on risque d'être accusés de faire la même chose ?

M. David Colon. Dans l'un de mes livres, j'explique en détail comment le Kremlin a développé une interprétation des événements de la fin de l'Union des Républiques socialistes soviétiques (URSS) basée sur une vision obsidionale : cette vision considère que l'ouverture sur le monde et une manipulation massive de l'information par les États-Unis ont conduit à l'effondrement soviétique. Bien que difficile à prouver pour cette période, il est indéniable que certaines initiatives américaines, comme celles d'Hillary Clinton sur la démocratie numérique, n'ont pas amélioré la situation. Le Département d'État américain a effectivement cherché à propager la démocratie et à déstabiliser les régimes non démocratiques. Même la France, en 2011, misait davantage sur Medvedev que sur Poutine.

Il est crucial de remettre les choses en perspective. Dans mon livre, j'ai analysé les archives disponibles sur les opérations menées par les États-Unis et la Central intelligence agency (CIA). À l'apogée de la guerre froide, ces opérations s'élevaient à 1 million de dollars par an, principalement pour traduire en ukrainien *1984* d'Orwell. En comparaison, les investissements russes atteignaient 3 milliards de dollars. Aujourd'hui, pour le Kremlin, l'Iran et la Chine, le champ informationnel est devenu le principal terrain de conflit. Le budget des médias d'État russes augmente de 13,5 % cette année, représentant des milliards de dollars d'investissements, en partie financés par notre dépendance au pétrole et au gaz.

Nous devons aider nos concitoyens à comprendre cette réalité et à éviter le whataboutisme kremlinien, qui met tout sur un pied d'égalité. Certes, il existe des interférences occidentales dans les espaces autoritaires mais elles sont minimales comparées aux interférences des régimes autoritaires dans les démocraties.

M. Arnaud Le Gall (LFI-NFP). Les ingérences russes et chinoises sont connues et inacceptables. Pour lutter efficacement, une approche globale est nécessaire. La situation aux États-Unis aurait dû nous alerter depuis longtemps, bien avant Trump.

Je m'interroge sur l'évolution économique. La bataille actuelle dans le capitalisme numérique, cœur du capitalisme mondial, se concentre sur l'accès aux données. L'Europe est un territoire convoité par les Chinois et les Américains. Quels sont les moyens concrets pour susciter une prise de conscience sur la nécessité d'une autonomie industrielle européenne dans ce domaine ?

Il n'existe pas seulement de la naïveté en Europe mais aussi de la duplicité. Chaque avancée est souvent sabotée en coulisses. Un exemple crucial concerne la recherche numérique civile, corrélée à une recherche numérique militaire à la hauteur : malgré les déclarations du ministre Lecornu, nous n'avons aucune garantie que le Fonds européen de la défense sera destiné à l'achat de matériel au sein de l'UE. Sans actions concrètes, les discussions resteront vaines.

M. Bernard Benhamou. Je reconnais les difficultés de coordination européenne dans ces domaines, exacerbées aujourd'hui par la présence d'acteurs agissant pour des intérêts étrangers au sein de l'Europe. La Hongrie en est un exemple flagrant.

Le projet de nomination de l'Américaine Fiona Scott-Morton à la direction de la concurrence de la Commission européenne était une aberration contre laquelle nous nous sommes battus. Il est inconcevable qu'une personne ayant travaillé avec Google et Microsoft puisse réguler ces plateformes en Europe.

Il existe une « imbécillité idéologique » du marché libre et non faussé, un ordolibéralisme qui rejette l'intervention publique. Pourtant, toutes les grandes plateformes chinoises et américaines utilisent massivement la commande publique. Aux États-Unis, le *Small business Act* oriente celle-ci vers les petites et moyennes entreprises (PME) depuis 1953. En Europe, nous nous l'interdisons au nom du marché, qui n'a manifestement pas résolu le problème.

Le diagnostic de Mario Draghi sur notre dépendance accrue, notre ouverture excessive, notre sous-investissement militaire est brutal mais nécessaire. Nous devons analyser lucidement ces questions, évitées jusque-là par résignation. Au début des années 2000, j'entendais souvent dans les ministères que « l'Internet, c'est américain, c'est fini ». J'étais choqué par cette attitude défaitiste.

Nous sommes une proie à deux niveaux : pour les données et économiquement. Je vous exhorte à la plus grande prudence concernant le contrôle des données mises à disposition d'acteurs extra-européens. Le *Health data hub* confié à Microsoft, avec des données ultrasensibles sur la santé des Français, en est un exemple.

Notre intérêt stratégique en tant que Français et Européens est de développer nos propres acteurs et écosystèmes, tout en conservant nos cerveaux. Nos données sont clairement ciblées et régulièrement volées, y compris par les Chinois lors de cyberattaques contre nos entreprises. Ces données servent à développer leurs propres systèmes d'intelligence artificielle, comme on le voit avec DeepSeek.

Plus grave encore, on nous vole nos cerveaux. La proportion d'ingénieurs et de physiciens français et européens travaillant dans la Silicon Valley sur le *data science* et le *machine learning* est considérable. Seules quatre entreprises européennes figurent parmi les cinquante premières mondiales dans les technologies, dont Schneider Electric pour la France, spécialisée dans la maîtrise de l'énergie. Nous devons accepter la création de géants européens, même si cela va à l'encontre du dogme bruxellois anti-concentration. Madame Vestager, malgré tout le respect que je lui porte, a une vision du siècle passé, craignant que la concentration n'entraîne une hausse des prix pour le consommateur.

Mme Laetitia Saint-Paul, présidente. Je vous remercie pour toutes vos interventions éclairantes.

La séance est levée à 13 h 10.

Membres présents ou excusés

Présents. – M. Pieyre-Alexandre Anglade, Mme Clémentine Autain, Mme Véronique Besse, M. Guillaume Bigot, M. Bertrand Bouyx, M. Jorys Bovet, M. Jérôme Buisson, M. Sébastien Chenu, Mme Sophia Chikirou, Mme Christelle D’Intorni, M. Alain David, Mme Christine Engrand, M. Olivier Faure, M. Marc de Fleurian, M. Nicolas Forissier, M. Julien Gokel, Mme Pascale Got, M. Michel Guinot, M. Stéphane Hablot, Mme Marine Hamolet, M. Alexis Jolly, Mme Sylvie Josserand, M. Arnaud Le Gall, M. Jean-Paul Lecoq, M. Vincent Ledoux, Mme Alexandra Masson, M. Laurent Mazaury, Mme Nathalie Oziol, M. Frédéric Petit, Mme Maud Petit, M. Kévin Pfeffer, M. Jean-François Portarrieu, M. Pierre Pribetich, M. Franck Riester, Mme Laurence Robert-Dehault, M. Jean-Louis Roumégas, Mme Marie-Ange Rousselot, Mme Laetitia Saint-Paul, Mme Sabrina Sebaihi, Mme Dominique Voynet, M. Lionel Vuibert

Excusés. – Mme Nadège Abomangoli, M. Gabriel Attal, Mme Eléonore Caroit, M. Marc Fesneau, M. Bruno Fuchs, M. Perceval Gaillard, M. François Hollande, Mme Brigitte Klinkert, Mme Amélia Lakrafi, Mme Marine Le Pen, Mme Mathilde Panot, M. Davy Rimane, Mme Michèle Tabarot, Mme Liliana Tanguy, M. Laurent Wauquiez, Mme Estelle Yousouffa