

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 économiques

– Audition de Mme Anne Le Hénanff, ministre déléguée
chargée de l'intelligence artificielle et du numérique. 2

Mardi 13 janvier 2026
Séance de 16 heures 30

Compte rendu n° 41

SESSION ORDINAIRE DE 2025-2026

**Présidence de
M. Stéphane Travert,**
Président



La commission des affaires économiques a auditionné Mme Anne Le Hénanff, ministre déléguée chargée de l'intelligence artificielle et du numérique.

M. le président Stéphane Travert. Notre commission a le plaisir de recevoir aujourd'hui Mme Anne Le Hénanff, ministre déléguée chargée de l'intelligence artificielle et du numérique, pour évoquer sa feuille de route et la politique mise en œuvre par le Gouvernement sur ces questions essentielles, tant pour la prospérité économique que pour la souveraineté de notre pays.

Madame la ministre déléguée, avant de vous céder la parole pour une quinzaine de minutes, je souhaite vous poser quelques questions. Plusieurs d'entre elles concernent l'intelligence artificielle (IA) et les suites que vous envisagez de donner au sommet sur la souveraineté numérique européenne, qui s'est tenu à Berlin le 18 novembre 2025.

Je m'interroge tout d'abord sur le financement public de l'intelligence artificielle. Le financement public fédéral américain de la recherche civile en IA représente plusieurs milliards de dollars par an, tandis que la Chine mobilise plusieurs dizaines de milliards de dollars, par le biais de l'État et d'instruments publics ou parapublics. Dans ce contexte, comment évaluez-vous la soutenabilité et la crédibilité des stratégies française et européenne en matière d'intelligence artificielle ? Des évolutions sont-elles prévues, alors que notre pays n'a mobilisé que 2,5 milliards d'euros (Md€) de fonds publics depuis 2018 ?

Lors du sommet sur la souveraineté numérique à Berlin, vous avez présenté la commande publique comme un levier de souveraineté numérique. Les achats publics représentent 15 % du PIB européen, mais une large part des services numériques utilisés par les administrations repose encore sur des solutions extra-européennes. Quelle stratégie souhaitez-vous promouvoir au niveau européen ? Où en est concrètement l'application de la préférence européenne dans les achats publics numériques ? Quels obstacles juridiques ou opérationnels freinent son déploiement effectif ?

Il serait intéressant que vous nous fassiez part de votre vision en matière de souveraineté et de dépendance aux infrastructures extérieures. L'essentiel des infrastructures dites « cloud », des modèles d'IA de grande taille et des semi-conducteurs avancés, est contrôlé par des acteurs américains ou asiatiques. Quelles sont les stratégies française et européenne visant à réduire ces dépendances critiques ? Sur quels maillons de la chaîne de valeur l'effort doit-il être prioritairement concentré, à court et moyen terme ?

S'agissant du numérique et de l'accès aux réseaux de communication, le « *New Deal* » mobile a permis de réduire la part du territoire métropolitain non couverte en 4G par un opérateur au moins : elle est passée de 11 % en 2018 à 1,4 % fin 2024. Près de 3 660 sites ont été mis en service dans le cadre du dispositif de couverture ciblée, sur un total de 5 122 zones identifiées. Compte tenu de ce résultat positif, comment expliquez-vous que des fragilités persistent dans certaines zones rurales, en particulier sur des axes de transport ? Quelles suites envisagez-vous pour consolider durablement la situation, notamment le développement possible d'un dispositif de couverture ciblée de seconde génération ?

Par ailleurs, le plan France très haut débit a permis d'atteindre, en 2025, un taux de couverture du territoire en fibre optique de 95 % et affiche la perspective d'atteindre 96 % en 2026 ; ce plan entre dans une phase de décaissements sans nouveaux engagements budgétaires significatifs. Comment le Gouvernement entend-il garantir la soutenabilité économique des réseaux d'initiative publique (RIP) dans les zones rurales, alors que la grande majorité d'entre

eux constatent des surcoûts par rapport à leur modèle économique initial et que la Cour des comptes pointe le risque qu'ils ne soient pas soutenables, à moyen terme, pour les collectivités ?

Enfin, alors que certaines zones du territoire demeurent difficiles à couvrir par les réseaux fixes ou mobiles terrestres, le recours aux technologies satellitaires apparaît de plus en plus comme une solution complémentaire pour assurer la continuité de la connectivité. Quelle stratégie le Gouvernement entend-il appliquer pour le développement et l'usage de solutions satellitaires dans ce but ? Comment cette stratégie s'inscrit-elle dans une logique de souveraineté numérique, eu égard notamment à la dépendance vis-à-vis d'acteurs extra-européens tels que Starlink, que nous devrions éviter si nous voulons préserver notre autonomie stratégique dans ce domaine ?

Mme Anne Le Hénanff, ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle, énergétique et numérique, chargée de l'intelligence artificielle et du numérique. Je vous remercie sincèrement de votre invitation : c'est une première pour moi de m'adresser à vous en tant que ministre déléguée chargée de l'intelligence artificielle et du numérique. Avant toute chose, permettez-moi de vous adresser mes meilleurs vœux pour 2026 : puissions-nous, ensemble, faire progresser les grands enjeux du numérique et de l'intelligence artificielle, afin d'en faire des outils utiles et humains, pleinement au service de nos concitoyens.

Cette audition est pour moi l'occasion, dans un premier temps, de vous présenter le bilan des trois premiers mois de mon action depuis ma prise de fonction, mais aussi les priorités et les grandes actions que nous conduirons dans les mois à venir, et de partager avec vous mes convictions profondes sur le numérique et l'intelligence artificielle.

Permettez-moi de poser d'emblée un constat simple : le numérique et l'intelligence artificielle sont devenus des sujets régaliens – l'actualité internationale nous le rappelle chaque jour. Le numérique est un nouveau champ de compétition, de contestation et parfois même de confrontation, qui recèle un potentiel immense. Il s'agit notamment de créer, d'innover, de rapprocher et de développer les filières françaises. Pour autant, ne soyons pas naïfs, il comporte aussi des risques réels qu'il nous faut comprendre et mesurer : des risques pour nos valeurs, pour nos démocraties et pour les plus vulnérables d'entre nous – en particulier, les enfants. Les choix que nous faisons aujourd'hui nous permettront de maîtriser notre destin numérique, qui s'incarne dans la notion centrale de souveraineté numérique.

C'est dans cet esprit que j'ai souhaité organiser mon action au sein du ministère, autour de quatre grands piliers. Le premier d'entre eux repose sur la maîtrise de nos fondations numériques, qui ne sont plus de simples supports techniques, mais sont devenues des infrastructures de souveraineté comparables à l'énergie, aux transports ou aux réseaux stratégiques. Les réseaux de télécommunications, les centres de données, les capacités de calcul et les infrastructures *cloud* forment l'ossature invisible de notre économie, de nos services publics et de notre cohésion territoriale. Ma conviction est claire : une nation qui ne maîtrise pas ses fondations numériques s'expose à des dépendances durables, parfois irréversibles. Maîtriser ne signifie pas tout produire seul, mais choisir, qualifier, sécuriser et piloter.

Le deuxième pilier vise à faire émerger des solutions européennes de rang mondial. Il est celui des solutions, des entreprises et des écosystèmes d'innovation. La souveraineté numérique ne se décrète pas : elle se construit pas à pas, par l'offre, par la capacité à faire émerger des entreprises compétitives, innovantes et capables de s'imposer sur les marchés européens et internationaux. À cet égard, la France dispose d'atouts considérables : des talents,

des chercheurs, des entrepreneurs et des acteurs qui s'imposent dans des secteurs clés. Notre responsabilité collective consiste désormais à réussir le changement d'échelle, ce qui suppose de la lisibilité réglementaire, de la stabilité, de l'accompagnement, mais aussi une mobilisation des commandes publique et privée. En effet, une souveraineté sans débouchés économiques n'est qu'un concept. Dans les prochaines années, nous devons faire du numérique et de l'IA des moteurs de croissance, de productivité et de compétitivité pour l'ensemble de notre économie.

Le troisième pilier consiste à sécuriser, réguler et protéger notre espace numérique. À mesure que le numérique pénètre tous les secteurs de notre économie et de notre société, il devient un espace de vulnérabilité. Cyberattaques, captation de données, espionnage économique, manipulation informationnelle : les menaces sont réelles, se multiplient et sont en constante évolution. Nous avons la responsabilité de bâtir un espace numérique sûr pour chaque utilisateur, fondé sur la prévention, la résilience et la capacité de réaction collective.

L'Europe joue un rôle central pour la protection des données et des réseaux, avec la directive *Network and Information Security*, dite « NIS 2 », en cours de transposition dans le cadre du projet de loi relatif à la résilience, des infrastructures critiques et au renforcement de la cybersécurité, dont l'examen en séance publique à l'Assemblée nationale est attendu.

Le quatrième pilier a pour but de placer l'utilisateur, le citoyen et la confiance au cœur de notre espace numérique. En France et en Europe, nous mettons le numérique au service de l'humain. Pour ce faire, il doit respecter les droits, les libertés et la dignité de celles et ceux qui l'utilisent. Cela implique de faire appliquer des cadres existants, notamment européens, et d'adapter nos outils à un environnement marqué par l'accélération des usages, des contenus et des technologies. La confiance est la condition de l'adhésion. C'est pourquoi nous sommes engagés pour faire du numérique et de l'intelligence artificielle des outils de progrès, de protection et de cohésion au service de tous.

Comment est-ce que j'agis concrètement pour mettre en œuvre ces quatre axes stratégiques ? Depuis octobre, nous avons voulu accomplir des actes clairs, à la hauteur des convictions que je viens de vous présenter. Le premier a concerné l'Europe de la souveraineté numérique : dès le mois de novembre s'est tenu à Berlin un sommet franco-allemand sur la souveraineté numérique, copiloté par l'Allemagne et la France.

Ce sommet a marqué une étape essentielle : nous y avons affirmé la nécessité de définir ce qu'est un service numérique européen. Une telle définition peut sembler technique, mais elle est fondatrice et marque une étape : elle conditionne notre capacité à faire émerger à l'échelle européenne une doctrine de souveraineté numérique et ouvre la voie, à terme, à une préférence européenne dans les marchés publics numériques. L'Allemagne et la France avancent désormais main dans la main, partageant une ambition : faire de la souveraineté numérique, en plus d'un principe, une réalité concrète incarnée par des choix politiques, économiques et industriels. Les groupes de travail opérationnels devront aboutir à des définitions utilisables, juridiquement solides et directement mobilisables au niveau européen. Nous travaillons afin d'être prêts ensemble, dans la perspective de la révision des directives européennes relatives aux marchés publics, prévue en 2026, qui soutiendra une vision franco-allemande.

Le deuxième chantier structurant consiste à mesurer nos dépendances pour mieux les réduire. L'observatoire de la souveraineté numérique, dont la création a été confiée au Haut-Commissariat à la stratégie et au plan, sous la responsabilité de M. Clément Beaune, aura une mission très claire : identifier, quantifier et qualifier nos dépendances numériques, filière par filière. Grâce à cet outil, nous pourrions répondre à des questions essentielles : où sommes-nous

dépendants et dans quelle mesure ? Quels sont les risques stratégiques qui en découlent ? Quels efforts devons-nous fournir pour réduire ces dépendances ? Il s'agit, là encore, de passer d'un discours général à des plans d'action précis, ciblés et assumés.

Le troisième axe de travail concerne les infrastructures, qui constituent le socle de toute souveraineté. La France peut être fière de sa politique publique concernant les réseaux. En matière de connectivité, la France se place sur la première marche du podium européen – c'est encore trop méconnu : 94 % des Français sont éligibles à la fibre et 99,5 % sont couverts par la 4G. Ces chiffres élevés sont le résultat d'années d'investissements, de partenariats avec les collectivités territoriales, qui ont joué un rôle majeur, de l'engagement des opérateurs et de la continuité de l'action publique. Grâce à une connectivité fibre et mobile de très haut niveau, la France attire des investissements massifs dans les *data centers*.

Lors du sommet pour l'intelligence artificielle, qui s'est tenu à Paris en février dernier, 109 Md€ d'investissement dans les *data centers* ont été annoncés ; sur les douze principaux projets, 75 % ont déjà sécurisé leurs sites en France. Je suis profondément fière de cette politique en faveur des *data centers*, qui s'appuie sur des compétences et des chercheurs français, crée des emplois en France et que nous devons amplifier en 2026.

Le quatrième axe de travail consiste à soutenir l'offre de solutions françaises et européennes en matière numérique, technologique et d'intelligence artificielle. Au mois de décembre, j'ai annoncé les nouveaux lauréats du programme French Tech. Celui-ci n'est pas symbolique : il structure des trajectoires de croissance, accompagne le changement d'échelle et donne de la visibilité à nos entreprises.

Dans le même esprit, nous avons engagé un travail de fond pour déployer des solutions d'intelligence artificielle au sein même de l'État. Avec mon collègue David Amiel, nous avons lancé un programme de déploiement de solutions fournies par l'entreprise Mistral dans les ministères, afin que l'administration devienne un acteur exemplaire de l'adoption technologique. Dans la même logique, nous finalisons actuellement avec le Premier ministre une circulaire structurante sur la commande publique numérique de l'État.

L'innovation, l'intelligence artificielle et le développement de la French Tech ne se jouent pas uniquement à Paris ou dans les métropoles, ce sont des réalités territoriales. Nous disposons de remarquables bassins d'innovation partout en France : la région Centre-Val de Loire, très en avance dans l'usage des données pour le pilotage des politiques publiques ; la région Pays de la Loire, qui utilise massivement les données et le numérique pour améliorer l'action publique locale ; la région Bretagne, qui est l'un des territoires les plus avancés en matière de cybersécurité. Nous devons valoriser ce qui se fait dans vos territoires et montrer que ces filières sont créatrices d'emplois, d'attractivité et de développement économique. Elles ne pourront se pérenniser et se développer qu'à condition que nous diffusions massivement l'intelligence artificielle. C'est tout le sens du programme Osez l'IA. Nous avons nommé plus de 500 ambassadeurs bénévoles répartis sur l'ensemble du territoire pour accompagner les acteurs publics, les associations, les citoyens et les entreprises dans leur compréhension et leur appropriation de l'IA.

Toutes ces actions reposent sur des choix budgétaires. Nous avons proposé de préserver, dans le projet de loi de finances (PLF) pour 2026, les crédits de France 2030 consacrés aux technologies de rupture, qui structurent nos filières d'avenir. Nous espérons la pérennisation du crédit d'impôt recherche (CIR), qui est un levier essentiel de compétitivité et d'innovation, et le maintien des dispositifs favorables aux jeunes entreprises innovantes.

L'effort budgétaire doit être collectif et le secteur du numérique prendra sa part, mais nous devons veiller à ne pas casser la dynamique engagée, qui a permis à la France de devenir un pays attractif en matière d'innovation technologique, de voir émerger des champions et de créer des emplois. Notre responsabilité consiste à consolider cette dynamique plutôt qu'à l'affaiblir.

Le cinquième axe concerne la cybersécurité, qui est un pilier régalien de notre souveraineté. La présentation de la revue nationale stratégique (RNS), en juillet 2025, a permis de dresser un diagnostic précis et actualisé des menaces cyber auxquelles nous sommes confrontés dans l'espace numérique. Les risques sont connus, identifiés et documentés. La responsabilité de l'État consiste désormais à organiser notre cyber-résilience. Pour cela, nous disposons de deux outils majeurs.

L'harmonisation européenne est le premier, en particulier la transposition de la directive NIS 2 dans le cadre du projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Cette transposition permettra de rehausser le niveau de cybersécurité de quinze mille entités en France, qu'elles soient publiques ou privées.

Le second outil est la stratégie nationale de cybersécurité, en cours d'élaboration. La cybersécurité passe par des outils techniques, mais surtout par la formation, la sensibilisation et l'apprentissage de la culture du risque par toutes les organisations et par les citoyens. Nous devons renforcer les moyens de l'Agence nationale de la sécurité des systèmes d'information (Anssi), structurer des référentiels solides, accompagner tous les acteurs et faire de la cybersécurité un réflexe national.

Le sixième axe de travail est la protection des mineurs et le renforcement de la confiance démocratique. Les questions sont nombreuses en ce domaine et nous devons y répondre collectivement. Comment voulons-nous organiser nos démocraties à l'ère des réseaux sociaux ? Comment protéger le débat public, les processus électoraux, mais aussi notre vie quotidienne ? Comment protéger les publics les plus fragiles, lutter contre la désinformation et les ingérences étrangères ? En ce domaine, le cadre européen, solide et exigeant, est unique au monde. La Commission européenne a commencé à l'appliquer réellement en prenant de premières sanctions dans le cadre du *Digital Services Act* (DSA), notamment l'amende de 120 millions d'euros (M€) infligée à la plateforme X, il y a quelques semaines. À ce titre, permettez-moi de saluer les travaux menés par des députés issus de tous les groupes, appelant l'Union européenne à être beaucoup plus réactive, en particulier face aux dérives observées de certaines plateformes.

Nous faisons face à de nouveaux défis liés à l'essor de certaines intelligences artificielles génératives. Nous devons donc aller plus vite, plus loin, et développer des capacités d'enquête, de sanction et de pénalisation plus innovantes. Cela passera par une protection renforcée des mineurs. Le Gouvernement s'est engagé dans la préparation d'un projet de loi instaurant une majorité numérique, dont l'objectif est clair : interdire l'accès aux réseaux sociaux aux mineurs de moins de quinze ans. Nous menons ce travail à l'échelle européenne, avec l'Espagne, Chypre, le Danemark, l'Irlande et d'autres pays souhaitant avancer à nos côtés.

Si je devais résumer en une phrase mon intervention et notre volonté, je dirais que notre ambition consiste à maîtriser notre destin numérique. Pour ce faire, une coordination internationale renforcée est nécessaire. La présidence du G7, en 2026, donne à la France l'occasion d'affirmer, avec ses partenaires, une ambition commune en matière de maîtrise du numérique, de cybersécurité et d'intelligence artificielle.

Par ailleurs, nous préparons le sommet international de l'intelligence artificielle qui se tiendra en Inde au mois de février, dans la continuité du sommet qui s'est tenu à Paris. Nous préparons ces échéances avec l'ensemble du Gouvernement, ainsi qu'avec des acteurs de la société civile, des entrepreneurs et des chercheurs. Notre objectif est clair : faire de ces événements des moments de convergence capables de produire des résultats concrets pour un numérique responsable au service de l'humain. Nous en sommes convaincus, la régulation du numérique ne peut être pleinement efficace qu'à l'échelle internationale ; à défaut, nous nous exposons à des contournements permanents. Vous l'aurez compris, le numérique est désormais non seulement un sujet régalien, mais aussi un sujet de diplomatie.

Monsieur le président, vous avez soulevé la question du financement de l'IA et évoqué la Chine et les États-Unis. La comparaison avec ces États est un peu délicate ; nous tentons de faire émerger en Europe et en France une IA qui nous ressemble, conforme à nos valeurs, ce qui n'est pas le cas de celles qu'ils proposent. La France a engagé 2,5 Md€ de fonds publics dans sa stratégie nationale ; mais si l'État a lancé la dynamique, il ne peut pas tout financer : le secteur privé doit prendre sa part. Le sommet consacré à l'IA a permis d'annoncer 109 Md€ d'investissement dans les *data centers* et nous accélérerons, dans les semaines à venir, le déploiement du plan Osez l'IA, afin de diffuser cette technologie dans tous les secteurs économiques.

En matière de commande publique, la ligne est claire : renforcer la maîtrise de l'État sur ses systèmes d'information, avec des exigences d'immunité au droit extra-européen. Cela passe notamment par la préférence européenne et par une définition précise de ce qu'est un service numérique européen.

Nous œuvrons au quotidien à la réduction de nos dépendances stratégiques, en commençant par les mesurer. La mission confiée au Haut-Commissariat à la stratégie et au plan permettra de les définir et de les réduire. S'agissant du *cloud*, nous avons défini une stratégie très claire de soutien aux fournisseurs européens respectueux de notre définition de la souveraineté numérique.

Le New Deal mobile est une politique publique coconstruite par l'État et les collectivités territoriales, qui est un grand succès. L'objectif de couverture ciblée prévoit cinq mille zones ; la prochaine occasion d'ajouter des obligations interviendra lors des attributions de nouvelles fréquences, autour de 2030. Une mission d'identification et de consolidation de ces fragilités d'ici à cette date a été confiée au Conseil général de l'économie.

Nous entendons les difficultés économiques relatives au *New Deal* mobile, au plan France très haut débit et aux RIP. Nous avons confié à l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) une mission d'évaluation de l'ampleur d'éventuels déficits. En fonction de ses conclusions, nous prendrons les décisions nécessaires permettant aux collectivités de réviser leur contrat, le cas échéant. Enfin, la France disposant déjà d'une excellente connectivité fixe et mobile, le recours aux satellites est résiduel, mais demeure utile en complément. L'enjeu stratégique majeur porte sur les fréquences. Nous œuvrons auprès de l'Union internationale des télécommunications (UIT) pour éviter toute concentration des fréquences au profit d'un acteur unique au niveau européen. Nous serons très présents dans les discussions relatives à tous ces enjeux, afin d'assurer la cohérence entre la continuité de la connectivité et la souveraineté numérique.

M. le président Stéphane Travert. Nous en venons aux interventions des orateurs des groupes.

M. Aurélien Lopez-Liguori (RN). France Travail, le ministère de l'intérieur et le ministère des sports : trois organismes publics, trois détenteurs de données sensibles et trois institutions « hackées ». Derrière ces attaques, des millions de nos concitoyens sont exposés, arnaqués, harcelés. Nos systèmes sont fragiles et chaque faille devient une opportunité pour des réseaux criminels. Personne ne prend ses responsabilités, personne n'est poursuivi et personne n'est mis en cause pour avoir laissé actives ces vulnérabilités. Quand les responsables de ces failles seront-ils punis ?

La directive NIS 2 est censée renforcer notre cybersécurité, mais sa transposition a déjà deux ans de retard. Le projet de loi correspondant n'a toujours pas été examiné en séance publique ; mercredi dernier, le ministre Roland Lescure a été incapable d'apporter une réponse claire quant au calendrier de son examen.

Toutefois, le problème est plus profond. Vous l'avez dit tout à l'heure : la cybersécurité ne se décrète pas et ne peut exister sans souveraineté ; les deux sont indissociables, ce sont les deux faces d'une même pièce. Nous ne semblons pas l'avoir compris, puisque nous sommes en passe de devenir, je le dis avec gravité, une colonie numérique américaine : la direction générale de la sécurité intérieure (DGSI) a renouvelé son contrat avec Palantir ; le Canadien CGI a été retenu pour assurer la cybersécurité des ministères ; Microsoft participe toujours au Health Data Hub : l'Assemblée nationale a choisi Bleu et Microsoft dans l'indifférence générale. Le loup est entré dans la bergerie, acclamé par les moutons eux-mêmes.

Dernièrement, l'Anssi a mis une couche supplémentaire en accordant le label SecNumCloud à S3NS, un acteur français, et à Google cloud. Concrètement, l'agence cyber française a estimé qu'utiliser Google comme *cloud* pour stocker des données sensibles ne posait aucun problème.

Alors que les tensions avec les États-Unis sont fortes, quel est le calendrier précis de la transposition de la directive NIS 2 ? Estimez-vous normal qu'une offre franco-américaine comme S3NS puisse obtenir le « sésame » ouvrant les portes des marchés les plus sécurisés de notre appareil d'État ? Quelle est la valeur de cette certification ?

Mme Anne Le Hénanff, ministre déléguée. Nous en avons discuté lors des débats devant la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité : le Gouvernement, soyez-en certain, prend ce sujet très au sérieux.

Toutes les conséquences des attaques qui ont eu lieu ont été tirées ; la cybersécurité est prise en compte dans les ministères comme dans toutes les organisations publiques. L'Anssi veille à la protection des systèmes d'information. Vous pouvez donc être rassuré sur ce point.

En ce qui concerne la transposition des directives NIS 2 et *Resilience of Critical Entities* (REC), ainsi que le *Digital Operational Resilience Act* (Dora), elle est prévue dans le cadre du projet de loi relatif à la résilience. C'est une obligation et nous la remplirons ; je ne peux pas vous donner à ce jour de date précise.

Vous m'interrogez aussi sur S3NS. La France a une stratégie IA, qui va nous permettre de produire et de collecter un nombre très important de données. Contrairement à vous, visiblement, je préfère des *data centers* situés en France et labellisés SecNumCloud, qu'ils soient d'État ou privés, plutôt qu'en dehors de notre territoire (ou pas labellisés). Ce label atteste

d'un niveau minimal de cybersécurité. J'ajoute que S3NS est détenu à 95 % par Thales. Il n'y a donc aucune inquiétude à avoir, ni sur la cybersécurité, ni sur la souveraineté.

Mme Nicole Le Peih (EPR). L'achèvement de la couverture numérique est un sujet vital pour l'avenir de nos territoires. L'ambition est claire, mais il demeure des obstacles très concrets, qui appellent une réponse commune. Si le déploiement progresse, le sentiment d'exclusion persiste ; là où la fibre semble s'arrêter au seuil des habitations, l'enjeu n'est plus seulement statistique, mais humain et opérationnel.

Comment garantir que la promesse de couverture devienne une réalité partout et sans exception ? Deux défis majeurs demandent une attention particulière : la résolution des raccordements complexes et l'aboutissement effectif du réseau. Trop de foyers restent sans solution à cause de fourreaux bouchés ou de poteaux à remplacer. Quelle est la stratégie pour débloquer ces situations rapidement et éviter que les usagers ne se sentent délaissés par le service public ? L'objectif doit être une couverture effective, et non seulement attestée par des indicateurs globaux. Quels leviers de pilotage peuvent être utilisés pour inciter des opérateurs à traiter l'habitat dispersé avec la même priorité que les zones denses ? Si nous voulons assurer l'attractivité de nos communes, il est indispensable de réussir ce pari de l'équité territoriale. Nous devons encourager cet effort pour que la qualité de service soit au rendez-vous partout et pour tous.

Je vous remercie aussi pour votre recherche de la maîtrise de notre destin numérique.

Mme Anne Le Hénanff, ministre déléguée. Depuis le lancement du plan France très haut débit en 2013, 42 millions de locaux ont été raccordés, soit 94 % des Français. C'est une prouesse industrielle ; notre pays est largement en avance par rapport à certains de nos voisins. La fibre est plébiscitée : 63 % des Français y sont déjà abonnés.

La Cour des comptes a récemment salué l'engagement de l'État, des collectivités territoriales et des entreprises – c'est souvent en équipe qu'on obtient les meilleurs résultats. Depuis 2013, 36 Md€ ont été alloués au plan France très haut débit, les financements publics (dont ceux des collectivités locales) représentant, quant à eux, 13 Md€.

Nous voulons continuer le développement de cette technologie aussi rapidement que possible ; notre objectif est que 100 % des foyers soient éligibles au très haut débit d'ici un an. Souvent, ce sont les derniers kilomètres qui sont les plus difficiles, soit parce que les habitats sont dispersés, soit parce qu'il y a des problèmes techniques – en particulier, la fibre remplace le cuivre, qui, à une certaine époque, était mis en pleine terre, alors qu'aujourd'hui, il faut installer des fourreaux.

Nous avons donc mis en place un dispositif d'aide, afin que les prix restent abordables : certains travaux, notamment sur les raccordements complexes, devront être financés par les particuliers et le prix peut être dissuasif. Notre plan permet d'obtenir des financements de 400, 800, 1 200 euros, selon la complexité du raccordement ; ce sont les opérateurs qui sont aux manettes. Nous ne laisserons personne au bord du chemin, soyez-en assurée.

M. René Pilato (LFI-NFP). Nous sommes entrés dans une nouvelle ère, celle du « techno-féodalisme », à savoir la mutation vers un capitalisme politique, financier, médiatique et technique où le pouvoir s'est transféré chez les géants de la Silicon Valley. Qui dit « féodalisme », dit suzerains et vassaux. Aujourd'hui, les suzerains ne tiennent plus leur pouvoir de la terre, mais de la propriété des infrastructures numériques, des données et des

algorithmes ; les vassaux sont ceux qui utilisent ces derniers, les subissent et finissent par se soumettre.

Quand le président Emmanuel Macron déroule le tapis rouge à M. Elon Musk, ce n'est pas l'affirmation d'une souveraineté, mais l'image d'un pouvoir politique qui quémade investissements et indulgence à celles et ceux qui contrôlent désormais l'infrastructure numérique mondiale. La naïveté atlantiste a endormi l'Union européenne pendant près de trente ans, mais l'enlèvement du président Nicolás Maduro et surtout les menaces du président Trump sur le Groenland, à qui on veut voler ses terres rares, doivent agir comme un électrochoc.

Nous ne pouvons plus faire confiance aux Américains, nous devons retrouver la pleine puissance de l'État français. Celle-ci passe non seulement par la souveraineté agricole et industrielle, mais aussi par la souveraineté numérique. La souveraineté n'est ni l'adaptation docile, ni la dépendance naïve ; elle passe désormais par une confrontation politique avec les empereurs du numérique et leurs technologies addictives qui veulent coloniser nos esprits et notre culture – ce que nous ne pouvons accepter.

Pourtant, le sommeil dogmatique perdure. Le 31 août 2025, la Cour des comptes a dressé un constat sans appel : « *L'ambition affichée par la France en matière de souveraineté numérique peine à être satisfaite, du fait notamment de la position prééminente des entreprises américaines et de la législation qui leur est applicable.* ». Les faits sont là : les infrastructures critiques de l'État, des messageries aux données de santé, passent massivement par des prestataires américains. L'usage interministériel des clouds « souverains » de l'État plafonne à 5 %. Nous saluons le partenariat entre l'armée de terre et MistralAI. Cependant, le chemin à parcourir reste encore si long.

Quand la France va-t-elle se donner les moyens politiques, industriels et budgétaires d'assurer sa souveraineté numérique, depuis les câbles sous-marins par le contrôle d'État d'Alcatel jusqu'aux logiciels libres et à un *cloud* souverain ? Êtes-vous prête à affronter les nouveaux souverains du numérique ou bien la France doit-elle accepter de rester leur vassal ?

Mme Anne Le Hénanff, ministre déléguée. Je ne partage pas votre analyse : à mon sens, nous ne sommes pas des vassaux ; en matière de souveraineté numérique, nous avons une vraie ambition.

Pour l'accomplir, nous devons d'abord réduire nos dépendances technologiques : nous y sommes. Notre ambition en matière de *cloud* est bien réelle : c'est là que sont sauvegardées nos données, c'est donc un point stratégique ; nous voulons les conserver sur notre territoire et les protéger avec un niveau de cybersécurité exigeant afin qu'elles ne soient pas soumises à des lois extraterritoriales.

Nous menons également une vraie politique industrielle de soutien à l'offre.

Enfin, nous avons une vision non seulement française, mais européenne, avec des règles et des valeurs qui nous sont propres.

Nous ne regardons pas passer les trains. Je le dis depuis mon arrivée au ministère, nous menons une vraie politique pour réduire nos dépendances technologiques et pour protéger nos données vis-à-vis des lois extraterritoriales.

M. Karim Benbrahim (SOC). Dans le développement de l'économie du numérique, la France, et plus largement l'Europe, accusent un retard préoccupant. Si, au cours du

XX^e siècle, notre pays a su développer des filières industrielles dans les secteurs en expansion (transports, énergie, aérospatiale, etc.), il a ensuite « raté » une série d'opportunités – les télécommunications, l'internet et, on peut craindre maintenant, l'intelligence artificielle. Ces domaines sont en effet largement dominés par des acteurs américains, concurrencés par des acteurs chinois.

Cette situation pèse de manière évidente sur nos emplois, mais aussi sur notre indépendance : nos données sont stockées, traitées, transportées par des infrastructures, des algorithmes et des *data centers* dont le contrôle nous échappe largement ; mais notre faiblesse ne se limite pas à cela, car une large part de l'information transite par des réseaux peu scrupuleux à l'égard de la qualité des contenus diffusés – je pense évidemment à X d'Elon Musk, à Meta, mais aussi à TikTok, qui a, par exemple, été le vecteur d'ingérences étrangères dans plusieurs scrutins sur le continent européen.

La décision récente de l'administration Trump d'interdire l'entrée sur le territoire américain à M. Thierry Breton et à quatre autres personnalités engagées pour une régulation des géants américains de la *tech* illustre le caractère central de cet enjeu. L'absence de réaction concrète de la part de la France et de l'Union européenne montre notre faiblesse.

L'enjeu énergétique ne doit pas non plus être négligé. Une étude de l'Agence de la transition écologique (Ademe) publiée la semaine dernière montre que, dans un scénario prolongeant la tendance actuelle, les besoins énergétiques liés à des centres de données situés à l'étranger mais répondant aux usages numériques des Français seraient multipliés par quatorze d'ici à 2050. Ce chiffre rappelle l'impératif de sobriété numérique, mais aussi la nécessité de relocaliser l'activité numérique sur notre territoire, qui dispose d'un *mix* électrique largement décarboné.

Au total, il est urgent de bâtir une véritable stratégie numérique et d'en faire un objectif stratégique national majeur. C'est l'un des axes du rapport Draghi. Malgré ces retards, la France dispose d'atouts réels pour faire émerger des champions de l'IA. Je pense aux jeunes chercheurs et jeunes ingénieurs qui, faute d'opportunités en France, vont exercer leur talent à l'étranger. Je pense aussi à notre électricité bas-carbone. Toutefois, l'écart avec nos concurrents américains et chinois s'accroît. Huit ans après la publication du rapport Villani sur l'IA, notre retard industriel s'est accru et notre dépendance s'est aggravée.

Notre pays et notre continent ne peuvent pas se contenter d'un rôle de régulateur d'innovations conçues ailleurs et imposées à nos économies. Nous avons besoin d'un projet national comme notre pays l'a connu dans le développement des industries du XX^e siècle que j'évoquais tout à l'heure. Or, je n'ai rien entendu dans votre propos liminaire qui soit de nature à changer réellement la donne. Quelle décision structurante le Gouvernement est-il aujourd'hui prêt à prendre pour inverser réellement cette trajectoire ?

Mme Anne Le Hénanff, ministre déléguée. Je n'aurai pas le temps de répondre à toutes vos questions et le ferai par écrit.

Je ne peux pas vous laisser dire que nous sommes en retard sur tout, que nous n'avons pas de vision. Ce n'est pas vrai. Nous avons pris du retard dans certains domaines, mais nous essayons de le combler – c'est le cas de la stratégie *cloud*. En revanche, nous sommes en très bonne position dans d'autres, comme l'intelligence artificielle ou le quantique, où nous disposons de pépites nombreuses, qu'on nous envie et qu'on tente de récupérer. En tout cas,

nous ne sommes pas ridicules par rapport au reste du monde et nous disposons de quelques grands acteurs.

Quant aux plateformes, nous ne fléchissons pas, nous ne laissons pas faire. Nous avons fait retirer des contenus et demandé la fermeture de certaines plateformes. Nous saisissons la justice dès que possible pour faire respecter le droit, tant par les utilisateurs que par les plateformes.

M. Jean-Luc Bourgeaux (DR). Le recours par l'État et de nombreux acteurs publics à des solutions de *cloud* majoritairement américaines, y compris pour l'hébergement de données sensibles, fait polémique. Ce débat, trop souvent abordé de manière binaire, mérite d'être clarifié et approfondi. Comment pouvons-nous garantir durablement la sécurité de nos infrastructures numériques alors que nous demeurons largement dépendants de technologies étrangères ? C'est notre souveraineté numérique et la protection des intérêts nationaux qui sont en jeu, dans un environnement géopolitique marqué par de fortes incertitudes.

Sur un plan plus opérationnel, quelles sont aujourd'hui les qualifications et certifications de référence permettant aux acheteurs publics de faire des choix éclairés pour que leurs données soient hébergées et traitées en toute sécurité ? Ces dispositifs vous paraissent-ils suffisamment lisibles, accessibles et adaptés aux besoins concrets des collectivités territoriales comme des administrations ?

Au-delà du cadre réglementaire se pose la question essentielle de la stratégie industrielle. Comment l'État français et l'Union européenne accompagnent-ils concrètement la montée en puissance d'acteurs français et européens du *cloud*, de la donnée et de l'intelligence artificielle, afin que la souveraineté numérique ne demeure pas un principe affiché mais devienne une réalité économique crédible, compétitive et durable ?

Mme Anne Le Hénanff, ministre déléguée. La protection des données est au cœur de notre réflexion – pas seulement en les considérant comme un risque, mais aussi comme une richesse pour notre capacité à innover et bâtir une souveraineté technologique européenne.

Le Gouvernement, notamment avec la stratégie nationale du *cloud*, s'est engagé à instaurer un cadre réglementaire protecteur, mais aussi à soutenir le développement d'un marché du *cloud* de confiance.

L'Anssi gère ainsi la qualification SecNumCloud. Ce référentiel de sécurité garantit la protection des systèmes d'information, ainsi que la confidentialité des données stratégiques en cas de cyberattaque : c'est un facteur de souveraineté essentiel. Cela protège notamment contre l'accès extraterritorial aux données. La sécurité est contrôlée sous un aspect technique – il faut être capable de faire face aux risques de cyberattaque –, sous un aspect opérationnel – il faut mesurer les risques d'accès illégitime – et sous un aspect juridique – quel est le droit applicable, notamment dans l'optique de protéger les données contre les lois extraterritoriales ?

Quatorze offres ont été qualifiées à ce jour – Cloud Temple, OVH et Orange, par exemple ; d'autres sont en cours de qualification. Ce processus de grande qualité recouvre 1 200 items différents : il faut beaucoup de temps et d'énergie et nous pouvons nous réjouir de disposer d'un tel niveau de sécurité.

Notre ambition est de développer des offres souveraines, y compris des offres hybrides, comme S3NS, développé par Thales avec Google.

La réunion est suspendue de dix-sept heures vingt à dix-sept heures trente-cinq.

Mme Louise Morel (Dem). Vous avez la responsabilité d'un ministère stratégique, aux prérogatives larges : les domaines du numérique et de l'intelligence artificielle sont porteurs d'innovation, mais ils suscitent aussi des questions.

S'agissant de la protection des données personnelles dans le cadre de l'intelligence artificielle, je voudrais revenir sur l'affaire Grok, qui illustre de manière particulièrement préoccupante les dérives possibles et dont s'inquiètent beaucoup de nos concitoyens. Sur le réseau social X, qui compte près de quinze millions d'utilisateurs en France, des photos et des contenus publics sont collectés par défaut afin d'entraîner cette intelligence artificielle et lui faire faire ce que l'on souhaite ; par exemple, certains utilisateurs demandent à Grok de mettre en bikini ou de dénuder des femmes. « *Si l'image est artificielle, le préjudice est bien réel.* », selon les termes de la commissaire à l'enfance Sarah El Haïry. Nos concitoyens découvrent ainsi, souvent sans l'avoir choisi, que leurs données, leurs images, parfois leurs visages, sont utilisés à des fins commerciales et technologiques.

Ajoutons à cela qu'en août dernier, plus de 370 000 conversations privées ont été divulguées, exposant des données sensibles et révélant l'insuffisance des protections.

L'Europe s'est dotée du règlement général sur la protection des données (RGPD). Force est de constater que ce cadre exigeant est souvent contourné par les acteurs numériques, qui testent en permanence les limites de la régulation.

Quelles actions le Gouvernement entend-il mettre en œuvre pour garantir le consentement explicite, éclairé et effectif des citoyens avant toute utilisation de leurs données par des systèmes d'intelligence artificielle ? Je sais que la justice s'est aussi emparée du sujet. Pourriez-vous nous rappeler le cadre de la loi ? Que pourrions-nous faire de mieux ? Quels moyens coercitifs, réellement dissuasifs, pourrions-nous mettre en place ?

J'aimerais aussi vous entendre sur la lutte contre les arnaques en ligne. La loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite loi « Sren », prévoit un filtre « anti-arnaque » afin de protéger les Français contre le *phishing* et les sites frauduleux. Or, contrairement à la volonté du législateur, le décret n'a toujours pas été publié. Pourtant, les chiffres sont alarmants : 79 % des Français sont les cibles d'escroqueries en ligne au moins une fois par mois, pour un préjudice estimé à 5,3 Md€ par an. Quand ce décret va-t-il être pris ?

Un autre aspect de cette loi concerne le blocage des sites pornographiques, auxquels deux millions d'enfants sont exposés chaque mois. Ce décret-là est paru : quelles sanctions ont déjà été prononcées contre les plateformes qui ne respectent pas leurs obligations ?

Mme Anne Le Hénanff, ministre déléguée. Merci pour ces questions sur des sujets sur lesquels je vous sais très engagée.

Le décret relatif au filtre anti-arnaque est en préparation. J'organise demain une réunion avec les députés qui ont travaillé sur la loi Sren afin de faire le point. Mon objectif est de publier ce texte très attendu. Il a été décidé à la mi-décembre que c'est l'Office anti-

cybercriminalité (Ofac) qui en serait chargé. Il reste des arbitrages à faire en matière de ressources humaines. Nous vous tiendrons au courant.

S'agissant de Grok, ce qui se passe est inadmissible. Vous avez vu que le Gouvernement réagit immédiatement à tous les incidents et saisit la justice pour demander non seulement le retrait des contenus illicites, mais aussi des sanctions – le code pénal punit les *deepfakes* à caractère sexuel de trois ans d'emprisonnement et de 75 000 euros d'amende. Il n'y a pas d'impunité. Vous pouvez compter sur nous pour faire appliquer la loi, qu'elle soit nationale ou européenne.

Mme Lisa Belluco (EcoS). Les collusions entre les Gafam, leurs patrons réactionnaires et le macronisme ne sont plus à démontrer : de l'accueil en grande pompe de MM. Mark Zuckerberg et Elon Musk à l'Élysée aux grandes embrassades avec M. Jeff Bezos, notre président ne cache plus son penchant pour les géants du numérique.

Ces huit dernières années ont été marquées par des choix lourds de conséquences pour la souveraineté de la France : la vente des données de santé des Français à Microsoft, avec le Health Data Hub, ou encore la permission d'installation débridée de centres de données partout en France.

Plus inquiétant encore, dans le domaine éducatif, une enquête récente de la cellule d'investigation de Radio France a révélé que des financements publics importants ont été accordés à des acteurs du numérique et à des chercheurs souvent proches des Gafam pour développer des outils numériques dans nos écoles. Cette enquête souligne que « *l'industrie du numérique bénéficie de subventions publiques importantes et développe des partenariats avec la recherche* » afin de favoriser l'introduction massive des écrans à l'école. Or, toujours selon ces journalistes, certains chercheurs liés à ces acteurs industriels auraient minimisé, voire contesté, les effets négatifs des écrans sur les enfants. Plus grave encore, un plan interministériel relatif à ces enjeux était prêt, mais aurait été délibérément bloqué par l'Élysée. Pourtant, le 31 décembre au soir, le Président de la République s'était engagé à « [protéger] *nos enfants et nos adolescents des réseaux sociaux et des écrans* ». S'agit-il de paroles en l'air ? La majorité numérique à quinze ans pour les réseaux sociaux, c'est une proposition un peu légère pour traiter ce sujet.

Les preuves scientifiques des impacts néfastes des écrans s'accumulent. Sédentarité, épidémie mondiale de myopie, manque de sommeil, trouble de l'attention et du langage : les effets délétères sur le développement des enfants ne peuvent plus être ignorés. Si le développement des technologies éducatives, les fameuses « *EdTech* », a été initialement justifié par l'objectif d'améliorer les performances scolaires, force est de constater que leur déploiement ne s'est accompagné d'aucune amélioration démontrée des résultats des élèves. L'essor des *EdTech* montre donc moins une efficacité pédagogique réelle que les logiques économiques et industrielles qui sous-tendent leur promotion au sein du système éducatif.

Dans un souci de transparence et d'indépendance de l'action publique en matière éducative, pouvez-vous revenir sur la nature, l'ampleur et les implications de ces révélations sur les collusions préoccupantes entre intérêts privés et acteurs publics ? Le Président de la République fera-t-il en sorte de tenir ses promesses et d'appliquer ce plan interministériel ? Et madame la ministre déléguée, agirez-vous dans ce sens ?

Mme Anne Le Hénanff, ministre déléguée. Je connais votre engagement sur ces sujets et je partage votre avis : protéger nos enfants est une priorité. Nous ne faisons pas rien !

Je m'appuie sur deux rapports : celui sur l'impact de l'exposition des jeunes aux écrans, remis en 2024 et qui formule une trentaine de propositions ; celui de MM. Arthur Delaporte et Stéphane Vojetta, intitulé « Influence et réseaux sociaux » et remis hier au Premier ministre, qui formule soixante-dix-huit propositions.

La majorité numérique ne vous paraît pas suffisante, mais c'est une première étape. Le Président de la République a également engagé, il y a plusieurs semaines, un débat national sur la démocratie à l'ère des réseaux sociaux. Plusieurs parlementaires sont aussi fortement engagés sur le sujet, par exemple la sénatrice Catherine Morin-Desailly et votre collègue Laure Miller.

Toutes nos actions doivent converger dans un grand projet de loi. Il y a aussi des aspects réglementaires.

M. Thomas Lam (HOR). Le numérique et l'intelligence artificielle sont au cœur de la transformation de l'action publique et de l'amélioration de notre compétitivité économique. À cet égard, la commande publique est un levier stratégique majeur. Par son effet d'entraînement sur l'ensemble de l'écosystème, elle oriente l'innovation et détermine notre capacité à préserver notre souveraineté numérique ainsi que la sécurité de nos données.

Je salue donc la volonté du Gouvernement du faire du *cloud* un outil de modernisation de l'action publique et de développer une offre de confiance souveraine capable de concilier performance et sécurité. Cette ambition s'inscrit dans une dynamique plus large, qui s'étend à l'échelle européenne. Les avancées permises par le sommet de Berlin ont en effet posé les bases d'une préférence européenne assumée et préfigurent la révision de la directive-cadre sur les marchés publics, qui permettra d'adapter nos règles aux exigences croissantes de souveraineté et de sécurité.

Dans ce contexte, la clarification du cadre de la commande publique numérique est un enjeu central. Elle doit permettre d'inscrire les achats numériques dans une doctrine partagée qui favorise la mutualisation des besoins, la réutilisation de solutions éprouvées et la limitation de la fragmentation des pratiques d'achat, tout en améliorant l'accès des entreprises françaises, notamment des PME et des start-up innovantes, aux marchés publics numériques.

La circulaire consacrée à la commande publique numérique dont vous avez annoncé la préparation vise notamment à repositionner la direction interministérielle du numérique et à clarifier les responsabilités de l'État acheteur ; nous nous en réjouissons. Pouvez-vous en préciser les grandes orientations ? Comment cette circulaire articulera-t-elle souveraineté, sécurité et efficacité opérationnelle pour les acheteurs publics ? Comment prend-elle en compte les échéances européennes à venir et la montée en puissance d'une offre numérique de confiance française et européenne ?

Mme Anne Le Hénanff, ministre déléguée. La commande publique est en effet un levier essentiel pour accompagner l'offre et renforcer notre autonomie stratégique ainsi que notre indépendance technologique. L'État et les collectivités doivent montrer la voie et privilégier des acteurs privés dès lors que l'offre existe.

La circulaire relative à l'achat public numérique est un guide d'achat « clés en main ». Elle rappelle les grands principes en matière de performance-métier, de sécurité, de souveraineté numérique et de coût et traduit une conviction forte : le soutien à l'offre. Il s'agit d'aider les très petites, petites et moyennes entreprises (TPE-PME) implantées sur l'ensemble

du territoire à franchir une étape de leur développement. Sa philosophie pourrait se résumer par la question suivante : pourquoi produire nous-mêmes ce qui existe sur le marché ? Nous comptons sur cette circulaire pour changer les pratiques d'achat public. Elle s'inscrit par ailleurs dans la perspective de la révision, en 2026, du « paquet » relatif à la commande publique européenne ; la France compte jouer un rôle moteur pour que celle-ci se tourne davantage vers l'offre privée.

M. le président Stéphane Travert. Nous en venons aux questions à titre individuel.

M. Aurélien Lopez-Liguori (RN). La loi Sren ayant été votée il y a deux ans, on pourrait s'attendre à ce qu'elle soit pleinement appliquée. Or, tous ses décrets d'application ne sont pas encore publiés.

C'est notamment le cas pour l'article 31, qui impose au Gouvernement de préciser les critères de souveraineté, notamment en ce qui concerne la détention du capital de l'opérateur du *cloud* utilisé pour héberger des données sensibles de l'État. Cet article hautement stratégique pour notre souveraineté numérique permettrait de réserver cette prestation à des acteurs européens. Vous qui attendiez impatiemment la publication de ce décret lorsque vous étiez députée, pouvez-vous, à présent que vous êtes au Gouvernement, nous indiquer quand elle interviendra ?

Mme Anne Le Hénanff, ministre déléguée. L'article 31 de la loi Sren, à laquelle je suis très attachée, a pour objet de renforcer la protection des données sensibles détenues par les fournisseurs de services *cloud*. Nous sommes si proches de l'aboutissement de la réflexion sur la doctrine applicable en la matière que j'aurais pu, à quelques jours près, vous annoncer la publication du texte que vous attendez.

Je me suis engagée à publier le plus grand nombre possible de décrets et je tiendrai parole ; mais nous devons prendre le temps d'examiner chaque article, car certaines dispositions peuvent être, par exemple, incompatibles avec le droit européen. En tout cas, pour ce qui est de l'article 31, nous sommes tout près d'aboutir et c'est une bonne nouvelle !

M. Jean-Luc Fugit (EPR). L'IA est souvent présentée comme un outil déterminant pour la gestion des réseaux électriques, qu'il s'agisse de la prévision de la demande, de l'intégration des énergies renouvelables ou de la maintenance prédictive. Par ailleurs, les *data centers* eux-mêmes consomment beaucoup d'électricité. Je souhaiterais donc savoir si vous êtes associée à l'élaboration du grand plan d'électrification des usages annoncé en décembre par le Premier ministre. Quelle est la stratégie de l'État concernant le déploiement de l'IA dans le secteur de la production et de la distribution d'énergie ? Je pense en particulier à la cybersécurité ; peut-être pouvons-nous, dans ce domaine, tirer des enseignements des événements survenus en Espagne, le 28 avril dernier.

Mme Anne Le Hénanff, ministre déléguée. Vous avez raison d'évoquer la question de l'énergie : nous en aurons besoin pour la filière *data centers* que nous avons l'ambition de créer. Nous avons la chance d'avoir, en France, une électricité décarbonée et disponible qui attire, du reste, de nouveaux investisseurs – je le constate chaque semaine.

Le règlement européen sur l'intelligence artificielle (RIA) prend en compte l'aspect environnemental de cette technologie et j'ai proposé à mes homologues de nous pencher, dans le cadre du « G7 numérique », sur la soutenabilité de l'IA.

À ce jour, la consommation électrique des *data centers* représente 2,5 % de la consommation électrique française mais, compte tenu du développement de ces infrastructures, cette part devrait assez rapidement doubler.

M. René Pilato (LFI-NFP). Je tiens à saluer votre volonté sincère de remonter la pente en matière de souveraineté numérique. Si toutefois, pour éviter de subir les colères ou les humeurs du président Trump, nous décidions, par exemple, de nous passer des puces Nvidia, nous devrions nous tourner vers le constructeur Huawei : nous restons, en tout état de cause, dépendants. A-t-on véritablement l'intention de maîtriser au niveau européen l'intégralité de la chaîne de valeur de l'IA, des terres rares jusqu'aux composants ?

Mme Anne Le Hénanff, ministre déléguée. Nous sommes tous attachés à la souveraineté numérique, mais je vous mentirais si j'affirmais que nous pouvons garantir notre indépendance dans l'ensemble du secteur, pour les *clouds*, l'IA, les *data centers*... L'objectif est plutôt de limiter notre dépendance à chaque maillon de la chaîne de valeur (composants, microprocesseurs, terres rares, etc.) et, lorsque ce n'est pas possible, de protéger nos réseaux et nos données.

M. Karim Benbrahim (SOC). Les opérateurs ont annoncé la fermeture, dans le courant de l'année 2026, des réseaux 2G utilisés par de nombreux services qui assurent la sécurité des citoyens, comme la téléassistance et la téléalarme des ascenseurs ou des équipements médicaux. Toutefois, à trois mois de l'arrêt d'un premier réseau, plus de 1 million d'équipements fonctionnent encore en 2G, selon les données de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep). Au mois de février, j'ai alerté vos services sur l'échéance de ces fermetures, mais ceux-ci ne semblent pas avoir pris la mesure du problème, qu'ils réduisent à sa dimension contractuelle. Sans remettre en question la pertinence technique de la fermeture de ces réseaux, je souhaite savoir quelles mesures vous entendez prendre pour garantir une transition sécurisée.

Mme Anne Le Hénanff, ministre déléguée. L'extinction des réseaux 2G et 3G, prévue respectivement pour 2026 et 2029, a été préparée ; les acteurs qui utilisent encore ces réseaux ont été prévenus de longue date par les opérateurs et l'Arcep s'assurera que les choses se passent bien. Du reste, 99,9 % des antennes relais équipées pour la 2G et la 3G le sont également pour la 4G, ce qui facilite la bascule technologique. En tout état de cause, nous ne pouvons pas maintenir des réseaux qui sont moins efficaces et consomment beaucoup plus d'énergie.

M. Jean-Pierre Vigier (DR). Lancé le 1^{er} juillet 2025, le plan Osez l'IA vise à accompagner toutes nos entreprises, en particulier les TPE-PME et les entreprises de taille intermédiaire (ETI), avec l'objectif ambitieux de rendre l'intelligence artificielle accessible et utile à tous d'ici à 2030. Toutefois, sur le terrain, la réalité est complexe. Ainsi, début 2026, seulement 26 % des TPE et PME déclarent utiliser l'IA, malgré la multiplication des *webinaires* et des initiatives de formation. Cette difficulté est encore plus sensible en milieu rural, où l'accès aux formations, aux infrastructures numériques et aux compétences spécialisées est plus limité. Aussi beaucoup d'entreprises peinent-elles à profiter du dispositif. Quelles mesures concrètes allez-vous renforcer pour que les TPE et PME, notamment celles des territoires ruraux, puissent réellement bénéficier de ces plans et former leurs équipes ?

Mme Anne Le Hénanff, ministre déléguée. Le plan Osez l'IA vise à diffuser l'intelligence artificielle partout, le plus rapidement possible, car nous sommes convaincus que cette technologie est un facteur de gain de productivité, notamment dans les TPE et les PME.

Notre objectif est que, d'ici à 2030, 50 % des TPE, 80 % des PME et des ETI et 100 % des grands groupes aient intégré l'IA dans leur fonctionnement.

À cette fin, nous avons désigné six cents ambassadeurs bénévoles, répartis sur l'ensemble du territoire pour y porter la bonne parole. Nous allons également mettre sur pied une « Académie de l'IA » chargée de former les chefs d'entreprise et développer divers dispositifs tels que les Pionniers de l'intelligence artificielle, conçue avec Bpifrance.

Cependant et j'en suis d'accord, cela doit aller beaucoup plus vite. Souvent, les difficultés sont dues au fait que les chefs d'entreprise, notamment de TPE, ne savent pas quel usage ils peuvent faire de l'IA. J'ai donc demandé à mes services de collecter des cas d'usage et de les diffuser largement auprès des chambres de commerce et d'industrie, des chambres de métiers et de l'artisanat, du Medef et de la Confédération des petites et moyennes entreprises (CPME).

Mme Cyrielle Chatelain (EcoS). J'ai de nombreux désaccords avec vous sur l'IA : on ne peut pas développer son utilisation sans s'interroger sur sa pertinence et son coût.

Je souhaite vous poser trois questions. Premièrement, des *data centers* doivent être construits dans ma circonscription, en Isère, par une entreprise, certes française, mais dont le créateur a vendu, il y a quelques années, ses infrastructures à une entreprise américaine, Vantage Data Centers. Qui plus est, cette entreprise bénéficiera d'investissements émiratis. En quoi cette opération renforcera-t-elle notre souveraineté ?

Deuxièmement, vous avez raison, nous pouvons être fiers que l'Europe ait été leader en matière de régulation, notamment grâce au règlement général sur la protection des données (RGPD). Toutefois, la proposition de règlement « omnibus » numérique pourrait remettre celui-ci en cause. Quelle est votre position sur ce point ?

Enfin, on parle beaucoup des réseaux sociaux. L'un d'eux est particulièrement nocif : je veux parler du réseau « X » d'Elon Musk et de son IA (Grok). Pourquoi êtes-vous toujours présente sur ce réseau ? Est-ce bien compatible avec nos valeurs ?

Mme Anne Le Hénanff, ministre déléguée. Lors du sommet sur l'IA, nous avons annoncé un investissement de 109 Md€ pour nous doter d'une véritable filière *data centers* et assurer ainsi notre autonomie en maîtrisant notre politique de la donnée. Il ne faut pas confondre investisseurs et opérateurs : ce n'est pas parce que des fonds américains investissent dans nos infrastructures que nous n'assurons pas notre souveraineté, laquelle s'évalue au niveau de la technologie qui équipe la machine. Or, celle-ci est bien française et soumise au RGPD.

Quant à l'« omnibus numérique », il vise à simplifier les règlements relatifs à l'IA et à la protection des données afin d'améliorer la compétitivité de nos entreprises vis-à-vis des géants américains.

Enfin, je suis effectivement présente sur X, mais n'utilise pas son IA générative.

Mme Nicole Le Peih (EPR). S'agissant de souveraineté numérique, les universités jouent un rôle clé en matière de formation, de recherche et d'innovation, notamment dans les domaines stratégiques de l'intelligence artificielle et de la cybersécurité. L'université Bretagne Sud tend à se renforcer dans ces champs prioritaires, au service des besoins nationaux et territoriaux. Toutefois, cette ambition ne pourra être pleinement réalisée sans le soutien durable de moyens humains – je pense en particulier à la création de postes d'enseignants-chercheurs.

Pourriez-vous préciser les mesures que l'État envisage de prendre pour accompagner les établissements, notamment grâce à la création de postes en intelligence artificielle et en cybersécurité, et la manière dont celle-ci pourrait s'inscrire dans un maillage équilibré du territoire breton ?

Mme Anne Le Hénanff, ministre déléguée. La formation des ingénieurs qui concevront l'IA à la française et à l'européenne est en effet un enjeu essentiel. C'est pourquoi nous investissons dans ce domaine, notamment dans le cadre de France 2030, et soutenons la recherche publique, en particulier dans des secteurs de rupture tels que le *cloud*, la cybersécurité ou l'IA. Quant à la création de postes d'enseignant-chercheur, elle relève des compétences du ministre de l'enseignement supérieur et de la recherche, mon collègue Philippe Baptiste, à qui je transmettrai votre question et que je vous invite à interroger à ce sujet.

M. Stéphane Buchou (EPR). Dans beaucoup de petites entreprises, l'intégration de l'intelligence artificielle se heurte à des obstacles liés à sa compréhension, à son coût et aux compétences nécessaires. Il est donc essentiel de les accompagner dans ce domaine tout en renforçant le rôle de l'humain, les savoir-faire et les emplois locaux. Il en va de leur compétitivité.

Le Gouvernement envisage-t-il de prendre des mesures concrètes pour renforcer cet accompagnement à l'échelle locale ? Comment comptez-vous faciliter l'accès de ces acteurs à des ressources, à des formations et à des experts en IA tout en garantissant que les bénéfices seront partagés équitablement entre les différents territoires ?

Mme Anne Le Hénanff, ministre déléguée. Je suis de ceux qui pensent que les entreprises qui rateront le virage de l'IA risquent de souffrir, voire de disparaître – c'est une réalité mondiale. Il faut donc les accompagner, former les salariés et expliquer aux chefs d'entreprise l'utilisation qu'ils peuvent faire de cette technologie. Les gains de productivité qu'ils peuvent en attendre permettront de dégager du temps qu'il faudra utiliser en confiant aux salariés des fonctions beaucoup plus valorisantes pour eux et pour le développement de l'entreprise.

Pour accompagner les entreprises, nous avons élaboré une véritable stratégie. Le plan Osez l'IA prévoit ainsi la désignation d'ambassadeurs qui seront répartis sur l'ensemble du territoire, la création d'une académie de l'IA destinée à former les chefs d'entreprise et le recensement, puis la diffusion, des cas d'usage positifs.

M. Nicolas Bonnet (EcoS). Ce n'est pas parce qu'un data center est physiquement en France que l'on maîtrise nécessairement les données qui y sont stockées. Si elles sont liées à des services développés par les Gafam, ces derniers ont la maîtrise de ces données, qui sont soumises au droit américain. Or, les Françaises et les Français utilisent massivement de tels services. Je souhaiterais donc savoir si vous avez élaboré une stratégie pour nous sortir de notre dépendance aux géants du numérique, ne serait-ce qu'en privilégiant l'utilisation des nombreux logiciels libres existants, qui nous permettraient d'assurer une véritable souveraineté numérique dans ce domaine.

En ce qui concerne l'IA, je suis effaré que vous vous en teniez à de telles généralités. Faisons confiance aux entreprises : elles savent mieux que nous si elles ont besoin de cette technologie – je ne suis pas certain que ce soit le cas du boulanger ou du plombier, par exemple. IA sans conscience n'est que ruine de l'âme. Donc, mettons-y un peu d'intelligence humaine...

Mme Anne Le Hénanff, ministre déléguée. En matière d'IA, je l'ai dit, ma politique est centrée sur l'humain. La conscience, nous l'avons aux niveaux national et européen.

Si les Américains investissent dans les *data centers* en France, cela ne me pose pas de problème. Du reste, il n'existe pas de *cloud* qui soit à 100 % américain : certains des acteurs sont forcément français. En tout état de cause, il faut privilégier une approche en termes de risque. Ainsi, la qualification SecNumCloud, qui s'applique aux données stratégiques sensibles, permet de protéger ces données de l'application d'un droit extraterritorial, quand bien même seraient-elles hébergées dans un data center financé par les Américains. C'est en empêchant que nos données partent à l'étranger que nous assurons notre souveraineté. Au demeurant, il n'y a pas, comme vous semblez le dire, d'investissement américain massif dans les *data centers* en France ; c'est de la désinformation.

Mme Cyrielle Chatelain (EcoS). Par deux fois, vous avez commis la même erreur. Notre collègue Nicolas Bonnet n'évoquait pas l'investissement dans les *data centers*, mais l'utilisation des données qui y sont stockées par les entreprises américaines qui en sont propriétaires. C'est un premier risque.

S'agissant du *data center* que j'ai évoqué dans ma question, une entreprise française – même si elle est située en Irlande – a acquis le foncier, mais ce sont des investissements des Émirats arabes unis qui, dans le cadre d'un accord conclu lors du sommet de l'IA, financent les machines, lesquelles appartiennent donc à l'entreprise émiratie.

Dans les deux cas, notre souveraineté est donc mise à mal.

Mme Anne Le Hénanff, ministre déléguée. Il y a différents types de *data center*. Lors du sommet sur l'IA, nous nous sommes engagés à développer une véritable filière dans ce secteur. Il se trouve que le coût de l'énergie et les engagements de l'État attirent les investisseurs étrangers. Nous n'avons rien contre eux. Il faut simplement que les acteurs qui sauvegardent leurs données dans un *data center* sachent dans quelles conditions elles y sont hébergées. La qualification SecNumCloud, comme le niveau d'exigence technique imposé par certains centres, permet de les protéger, en particulier si elles sont sensibles et stratégiques. Toutes les données sauvegardées dans des équipements financés par des étrangers ne sont donc pas soumises à un droit extraterritorial. En tout état de cause, nous souhaitons que les données françaises restent en France.

Je vous remercie pour ces échanges passionnants. Il était important pour moi de vous présenter notre ambition en matière d'intelligence artificielle et de numérique. Notre filière IA se porte bien. D'autres sont en cours d'amorçage – je pense au quantique et à la cybersécurité, par exemple. J'aurai toujours plaisir à venir vous rendre compte des avancées dans ces domaines.

M. le président Stéphane Travert. Nous ne manquerons pas de vous solliciter, car des rendez-vous importants sont annoncés concernant le numérique.

Membres présents ou excusés

Commission des affaires économiques

Réunion du mardi 13 janvier 2026 à 16 h 30

Présents. – M. Karim Benbrahim, M. Jean-Luc Bourgeaux, M. Stéphane Buchou, M. Jean-Luc Fugit, M. Thomas Lam, Mme Nicole Le Peih, M. Aurélien Lopez-Liguori, M. Nicolas Meizonnet, Mme Louise Morel, M. René Pilato, M. Vincent Rolland, M. Stéphane Travert

Excusés. – Mme Valérie Létard, M. Philippe Naillet, M. Stéphane Peu, Mme Marie-Agnès Poussier-Winsback, M. Richard Ramos

Assistaient également à la réunion. – Mme Lisa Belluco, M. Nicolas Bonnet, Mme Cyrielle Chatelain