ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Compte rendu

Commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France

Jeudi
30 avril 2026
Séance de 10 heures 30

Compte rendu n° 36

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à dix heures trente-cinq.

M. le président Philippe Latombe. Mes chers collègues, nous recevons à présent M. Henri d'Agrain, délégué général du Cigref (Club informatique des grandes entreprises françaises). Au cours de nos auditions, il a souvent été question d'une étude sur la dépendance technologique européenne estimant que 83 % des achats de services *cloud* et logiciels des entreprises européennes sont adressés à des acteurs américains, soit environ 265 milliards d'euros par an. Pouvez-vous présenter cette étude et sa méthodologie ? Comment rapatrier ces services en France ?

Je vous remercie de nous déclarer tout intérêt public ou privé de nature à influencer vos déclarations. Auparavant, je vous rappelle que l'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires impose aux personnes auditionnées par une commission d'enquête de prêter serment de dire la vérité, toute la vérité et rien que la vérité.

(*M. Henri d'Agrain prête serment*).

M. Henri d'Agrain, délégué général du Club informatique des grandes entreprises françaises. Je vous remercie de me recevoir aujourd'hui. À titre liminaire, je souhaite préciser mes intérêts. Je suis personnalité qualifiée au sein d'une commission extra-parlementaire, la Commission supérieure du numérique et des postes (CSNP), présidée par le sénateur de l'Isère, M. Damien Michallet. Pour le reste, je suis un ancien officier de la marine nationale et, depuis une dizaine d'années, délégué général du Cigref.

Avant d'entrer dans le fond, permettez-moi de rappeler brièvement que le Cigref est une association loi 1901, à but non lucratif, sans activité commerciale. Ses membres sont les grandes entreprises françaises ou de racines françaises, ainsi que de grandes administrations publiques françaises, en leur qualité d'utilisatrices de produits et de services numériques. Le Cigref porte donc la voix des grandes organisations publiques et privées utilisatrices du numérique en France.

Le propos que je tiens aujourd'hui s'appuie sur les travaux d'intelligence collective conduits avec nos adhérents, que je représente aujourd'hui. Mon intervention se limitera volontairement aux domaines que nous connaissons et sur lesquels nous travaillons, en particulier le marché B2B des logiciels et des services cloud à usage professionnel. Je n'aborderai pas le marché B2C, pour lequel le Cigref ne dispose pas d'une expertise spécifique distincte de celle de tout usager, même si les opérateurs peuvent parfois être les mêmes.

Venons-en à la notion de dépendance technologique telle qu'elle est perçue par les adhérents du Cigref. Il faut d'abord rappeler que toute organisation s'inscrit dans un écosystème de dépendances : dépendance à l'égard des actionnaires, des collaborateurs, notamment pour les compétences critiques, dépendance vis-à-vis de partenaires et de fournisseurs de toute nature. La dépendance technologique, en elle-même, n'est donc ni anormale ni honteuse ; elle constitue le cadre ordinaire de fonctionnement de toute entreprise ou administration.

En revanche, lorsque l'on est dépendant, il est indispensable de disposer d'une cartographie rigoureuse des risques induits par ces dépendances. Cette démarche vise ainsi à réduire les menaces pesant sur la résilience de l'organisation, c'est-à-dire sa capacité à absorber, encaisser et surmonter des chocs ou des perturbations de toute nature.

Or, depuis des décennies, les conséquences systémiques des dépendances numériques des entreprises, des administrations publiques et, plus largement, de notre économie ont été largement sous-estimées. Elles ont été insuffisamment analysées et souvent minimisées par de nombreux décideurs, qu'ils soient économiques ou politiques. Dans un contexte de conflictualité croissante, la résilience numérique est ainsi devenue une préoccupation de tout premier plan pour l'ensemble des membres du Cigref.

Cette prise de conscience ne date pas d'hier. Elle s'inscrit dans le prolongement de travaux réglementaires importants, tels que le règlement sur la résilience opérationnelle numérique du secteur financier (Dora) ou la directive NIS 2. Ces textes ne traitent pas uniquement de cybersécurité au sens strict, mais bien de résilience, entendue comme la maîtrise des dépendances stratégiques. Dora vise explicitement la résilience opérationnelle, notamment dans le secteur financier, et constitue aujourd'hui un standard de réflexion qui s'étend progressivement à l'ensemble des secteurs critiques. La définition de la résilience qu'il propose nous semble pertinente pour être appliquée à tous les secteurs confrontés aux enjeux de dépendance numérique.

Lorsque l'on parle de dépendance technologique, il est essentiel d'en mesurer les conséquences majeures. Nous en identifions trois catégories principales, communes aux organisations publiques et privées. La première est d'ordre économique. Lorsqu'une organisation se trouve en situation de dépendance et de verrouillage technologique, elle offre à son fournisseur la possibilité d'exploiter cette dépendance de manière abusive, qui se traduit généralement par des hausses tarifaires excessives. Ce phénomène est aujourd'hui massif. Vous avez évoqué la première étude Asterès que nous avons publiée en avril 2025, mais une seconde étude sera publiée à la mi-mai 2026. Elle portera spécifiquement sur les hausses tarifaires à l'horizon de cinq ans, jusqu'en 2030-2031, et sur leurs conséquences macroéconomiques pour l'économie européenne. Il s'agit là d'un sujet de préoccupation majeure pour nos adhérents, car il touche directement à la captation de valeur par des acteurs dominants. Ces conséquences sont aujourd'hui exploitées de manière massive.

La deuxième conséquence est d'ordre juridique. Les données, qu'elles soient personnelles ou non, ainsi que les traitements associés, sont souvent hébergés dans des infrastructures *cloud* soumises à des législations non européennes. Cela ouvre la voie à des accès légaux et secrets par des puissances étrangères. L'exemple le plus connu est celui de la section 702 du *Foreign Intelligence Surveillance Act* (Fisa) américain. La Chine dispose d'un dispositif comparable avec sa loi sur le renseignement du 27 juin 2017. Ces cadres juridiques posent de lourdes questions en matière de confidentialité des données. Ils peuvent également être mobilisés dans des stratégies de sanctions, comme l'illustrent certains cas récents, notamment ceux des magistrats de la Cour pénale internationale.

La troisième conséquence est d'ordre géopolitique. Dans un monde marqué par des tensions exacerbées, ces dépendances systémiques peuvent devenir des leviers de contrainte ou de rétorsion, utilisés pour influencer le comportement d'États rivaux ou même alliés.

À ce stade, je souhaite attirer votre attention sur une illusion dangereuse, parfois relayée par certains observateurs. Je pense notamment à l'idée déployée par Mario Draghi dans son rapport, selon laquelle l'Europe aurait perdu la bataille du *cloud* et devrait désormais se concentrer sur celle de l'intelligence artificielle. Cette vision est trompeuse : l'intelligence artificielle est un service *cloud* comme un autre ; il n'y a pas d'IA sans infrastructures cloud. Imaginer une stratégie d'IA indépendante des infrastructures relève de la même logique que certaines doctrines industrielles passées, comme la doctrine des entreprises sans usines (« *fabless* ») de Serge Tchuruck dans les années 1990, qui ont contribué à accélérer la désindustrialisation de l'Europe.

Il n'existe pas de stratégie « *serveurless* » viable. L'entraînement et le déploiement des modèles d'IA sont indissociables des infrastructures matérielles. Lorsque l'on observe les coûts complets, on constate une répartition de l'ordre de 80-20 : 80 % relèvent des infrastructures, 20 % du développement des modèles.

Une économie avancée ne peut durablement accepter que 80 % de sa production industrielle soit localisée en Asie et 80 % de ses services numériques aux États-Unis. Une telle dynamique serait insoutenable. Il n'y a pas d'avenir pour une économie européenne qui renoncerait à la maîtrise de ses infrastructures numériques critiques.

Par ailleurs, puisque ce point figurait dans votre questionnaire, je souhaite revenir sur la notion de souveraineté. Du point de vue du Cigref, il est impératif de distinguer clairement deux niveaux d'analyse : le niveau microéconomique et le niveau macroéconomique. Le premier relève des entreprises elles-mêmes. Il engage directement la responsabilité des dirigeants, des directions du numérique et des systèmes d'information. Leur mission consiste à développer la résilience numérique de leur organisation à partir d'analyses de risques qui leur sont propres. Ces risques sont par nature hétérogènes ; ils varient selon les secteurs d'activité, les implantations géographiques, les chaînes de valeur.

Le second niveau est macroéconomique. La responsabilité revient à l'État et à l'échelle pertinente aujourd'hui, aux institutions européennes. Il relève des politiques publiques de créer des cadres de souveraineté, à travers la réglementation, les investissements stratégiques, la commande publique et les politiques industrielles.

Sur ce point, la position du Cigref est claire et rigoureuse : la souveraineté est un attribut exclusif de l'État. Il suffit de se référer à la définition du dictionnaire de l'Académie française ou au rapport remarquable du Conseil d'État sur la souveraineté publié en 2024. La souveraineté désigne la compétence exclusive de l'État à exercer ses responsabilités sur une population et un territoire, compétence limitée uniquement par les engagements internationaux qu'il a librement consentis.

Dans ces conditions, parler de « solutions souveraines » ou de « *cloud* souverain » relève bien souvent d'une forme de paresse intellectuelle. Rien ne justifie que, dans le champ numérique, on s'écarte de cette définition fondamentale. C'est pourquoi le Cigref parle, pour les entreprises, de résilience, et appelle les États et les institutions européennes, dans le cadre de leurs compétences respectives, à mettre en œuvre de véritables politiques de souveraineté dans le champ de l'économie numérique.

Or, force est de constater qu'à ce jour, ces politiques sont largement inexistantes ou très insuffisamment mises en œuvre, en particulier sur le marché B2B des logiciels et des services *cloud*, qui constitue le cœur de notre champ d'observation. Prenons l'exemple de la régulation de la concurrence. Sur ce marché, il existe manifestement un défaut d'action publique, puisqu'à de rares exceptions près, les autorités de concurrence et les pouvoirs publics sont restés largement inertes. Le rachat de VMware par Broadcom en constitue une illustration emblématique. Ce rachat a été annoncé en mai 2022. Or, dès septembre 2021, le Cigref avait saisi l'Autorité de la concurrence sur les pratiques abusives de Broadcom à la suite du rachat de CA Technologies et de Symantec Enterprise. Malheureusement, cette saisine n'a jamais été instruite.

En 2022, nous avons alerté la Commission européenne et les autorités françaises : si Broadcom rachetait VMware, les mêmes mécanismes se reproduiraient. À l'époque, tous les adhérents du Cigref, publics comme privés, étaient clients de VMware d'une manière ou

d'une autre. Le risque de position ultradominante était donc évident. Les faits nous ont malheureusement donné raison. En 2024 et 2025, nous avons observé des hausses tarifaires massives, des modifications unilatérales des modèles de licences et de tarification, et une véritable prédation sur l'économie européenne, dans un climat d'atonie quasi totale des pouvoirs publics, et notamment des autorités de concurrence.

Dès lors, une politique de souveraineté, sur ce marché où 264 milliards d'euros sont transférés chaque année vers les États-Unis et où 83 % des achats européens de logiciels et de services cloud B2B sont captés par des acteurs américains, devrait commencer par l'application effective du droit de la concurrence. Ce serait là un premier pilier concret d'une politique de souveraineté. En l'absence de régulation, la plupart des opérateurs dominants exploitent de manière systématique et abusive les situations de dépendance économique et technologique de leurs clients.

Un autre exemple de ce vide régulatoire est fourni par le règlement sur les marchés numériques (DMA). Celui-ci identifie dix « *core platform services* », parmi lesquels figurent les services *cloud*, en dépit d'un intense lobbying visant à les en exclure. Pourtant, lorsque la Commission européenne a désigné les *gatekeepers* le 6 septembre 2023, aucun acteur n'a été désigné pour les services cloud. Nous sommes dans cette situation depuis plus de deux ans.

En novembre dernier, à Berlin, la Commission a annoncé l'ouverture d'enquêtes sur AWS et Microsoft, ainsi qu'une réflexion sur les modalités de désignation de *gatekeepers* dans les *cloud services*. Mais au regard des délais observés et de la rapidité des évolutions technologiques, il est permis de douter.

Les positions dominantes continuent de se renforcer, notamment par l'intégration de nouveaux services comme les outils d'intelligence artificielle, qui sont eux-mêmes des services *cloud*. Je pourrais multiplier les exemples. Mais le message essentiel est celui-ci : il n'y aura pas d'avenir pour l'économie européenne si elle ne se dote pas d'une véritable industrie du numérique. De fait, il n'y a pas d'avenir pour l'économie européenne si celle-ci ne dispose pas de sa propre industrie du numérique.

Par ailleurs, il me semble que le regard porté sur la régulation du numérique entre l'Europe et les États-Unis a profondément évolué, même si cette évolution n'est pas toujours perçue clairement. On entend souvent l'idée selon laquelle les États-Unis innoveraient tandis que l'Europe se contenterait de réguler. À mon sens, cette formule est trompeuse, car elle repose sur une lecture biaisée de ce que recouvre réellement la notion de régulation.

En Europe, la régulation est traditionnellement conçue avec deux objectifs primaires : garantir des prix bas pour le consommateur et assurer la protection de la vie privée. Lorsque l'on observe la situation américaine à travers ces lunettes européennes, on en conclut rapidement que les États-Unis ne régulent pas. Or cette conclusion est erronée : il existe bien une régulation aux États-Unis, mais elle repose sur un objectif fondamentalement différent, qui concerne la préservation et le renforcement de la puissance nationale.

L'industrie de la technologie et du numérique constitue l'un des quatre piliers de la puissance et de l'hégémonie américaines dans le monde. Cette réalité structure la manière dont les États-Unis conçoivent leur régulation. De ce point de vue, il serait souhaitable que l'Europe accepte, au moins ponctuellement, d'adopter les lunettes du régulateur américain lorsqu'il s'agit de penser l'avenir de son industrie numérique et la résilience de son économie.

Je souhaite conclure ce propos introductif en revenant sur les principaux enseignements de l'étude que nous avons publiée en avril 2025 sur le coût de la dépendance technologique européenne. Les chiffres sont connus, mais il me semble utile de les rappeler. Chaque année, 264 milliards d'euros sont dépensés sur le marché B2B des logiciels et des services *cloud* auprès d'entreprises américaines. Cela représente 83 % des achats réalisés par l'économie européenne sur ce segment.

Environ 80 % de la valeur ainsi générée est créée aux États-Unis, ce qui permet d'y soutenir près de 1,9 million d'emplois directs, indirects et induits. L'étude se concluait par une projection volontairement prudente : si, d'ici 2035, l'Europe parvenait à rapatrier seulement 15 % de ces dépenses vers des opérateurs européens, cela pourrait permettre la création de plus de 450 000 emplois sur le continent. Ce chiffre est loin d'être marginal.

Je tiens à préciser que cette étude ne s'inscrit absolument pas dans une logique d'éviction des technologies américaines. L'objectif était de mettre en évidence une dynamique de dépendance croissante, qui s'opère au détriment de l'économie européenne. À titre de comparaison, les 264 milliards d'euros consacrés chaque année aux services numériques américains sont du même ordre de grandeur que les dépenses européennes annuelles en gaz et en pétrole, qui s'élèvent à environ 350 milliards d'euros.

Vous m'avez également interrogé sur la méthodologie de cette étude. Il convient d'abord d'expliquer pourquoi nous avons confié ce travail au cabinet Asterès. En 2023-2024, lorsque nous avons cherché à quantifier le coût de ces dépendances, nous avons constaté qu'aucune donnée consolidée n'existait. Ni Eurostat, ni la Banque centrale européenne (BCE), ni le FMI ne disposaient de chiffres permettant d'identifier précisément le montant des achats européens de services numériques auprès d'entreprises américaines.

Cette lacune s'explique par la nature même de ces flux. Lorsqu'une entreprise européenne achète un service numérique à un acteur américain, il s'agit juridiquement d'un échange intra-européen, puisque les filiales sont implantées en Europe. Les revenus sont ensuite rapatriés vers les États-Unis sous forme d'investissements directs étrangers (IDE), le plus souvent via des structures localisées en Irlande, mais également aux Pays-Bas ou au Luxembourg, pour des raisons d'optimisation fiscale. La première conclusion de notre étude n'est donc pas tant le chiffre de 264 milliards que le constat suivant : il n'est pas normal que l'Europe ne dispose d'aucune donnée fiable sur un phénomène de cette ampleur.

Ensuite, la méthodologie retenue repose sur une analyse microéconomique approfondie. Six entreprises issues de secteurs différents ont été interrogées, avec un examen détaillé de leurs factures, de leurs contrats et de leurs usages. Les économistes d'Asterès ont ensuite extrapolé ces données à l'échelle macroéconomique européenne à l'aide de leurs modèles. Des vérifications de cohérence ont été menées, notamment par comparaison avec les études semestrielles de conjoncture de Numeum et les données du marché du logiciel. De fait, les ordres de grandeur obtenus apparaissent robustes.

Nous publierons à la mi-mai 2026 une deuxième étude, également réalisée avec Asterès, portant sur l'impact macroéconomique des hausses tarifaires observées sur le marché du logiciel et des services cloud. Cette étude s'appuie sur un échantillon élargi de cinquante-quatre entreprises européennes, incluant des acteurs français, allemands, néerlandais et belges. Elle analyse les hausses tarifaires constatées depuis cinq ans et projette leur évolution à l'horizon 2030-2031.

Les premiers résultats sont particulièrement préoccupants. Alors que l'inflation « normale » des prix des logiciels devrait se situer autour de 2,7 %, nous observons une hausse effective proche de 9 %, soit un facteur trois. Les projections indiquent une poursuite de cette dynamique entre 9 % et 12 % par an sur les cinq prochaines années. À ce rythme, une facture double en moins de huit ans.

Si rien ne change, les 264 milliards d'euros actuels pourraient dépasser 500 milliards à l'horizon 2032, à périmètre constant. Or 93 % des directions interrogées estiment que ces hausses ne sont pas justifiées par des gains de productivité équivalents. Nous évaluons donc le surcoût annuel moyen pour l'économie européenne à 68 milliards d'euros, dont 45 milliards d'euros repartiraient directement vers les États-Unis chaque année.

Sur le plan macroéconomique, Asterès estime que ces hausses pourraient entraîner une perte de 0,3 point de PIB par an pour l'économie européenne d'ici 2030 et la destruction d'environ 660 000 emplois. Je ne suis pas économiste et je ne prétends pas juger de la pertinence ultime de ces modèles, mais Asterès est reconnu pour son sérieux et ses travaux font référence.

Enfin, je souhaite répondre à une remarque relative à une supposée naïveté passée des dirigeants européens concernant l'accès des agences de renseignement américaines aux données des citoyens non américains. Il ne s'agissait pas tant de naïveté que d'un impensé ; la question ne se posait pas réellement il y a dix ans. Elle aurait sans doute dû se poser plus tôt. En revanche, depuis trois à cinq ans, je constate une prise de conscience très nette chez nos adhérents. Ainsi, les grandes organisations disposent désormais, pour la plupart, de stratégies visant à conserver leurs données les plus sensibles et stratégiques sur leurs propres infrastructures. Elles utilisent les outils des grands fournisseurs internationaux en pleine connaissance de cause, mais sans y exposer leurs actifs informationnels critiques.

Cette prise de conscience se heurte toutefois à une limite : l'incapacité actuelle des institutions européennes à adopter des cadres juridiques réellement protecteurs des données sensibles et stratégiques des entreprises. Les hésitations et revirements observés depuis 2023 sur la certification européenne pour les services de cloud (EUCS) et notamment le niveau High +, en témoignent.

M. le président Philippe Latombe. Je vous remercie pour ce panorama. Le chiffrage que vous avez donné, issu de votre première étude, a fréquemment été cité lors des différentes auditions. Vous la prolongez cette année avec une autre étude portant sur les augmentations tarifaires, à isopérimètre, c'est-à-dire hors IA.

M. Henri d'Agrain. Des projections ont effectivement été établies, nous sommes actuellement au stade de la vérification, avant la prochaine publication.

M. le président Philippe Latombe. À périmètre équivalent de l'étude que vous aviez menée en 2025, vous projetez les augmentations tarifaires. Vous indiquez qu'elles ne sont pas justifiées par une augmentation de la productivité des entreprises clientes. Cependant, à un moment ou à un autre, elles doivent avoir une justification pour l'entreprise qui fournit son produit. Comment l'expliquez-vous ? S'agit-il de pouvoir financer d'autres investissements, par exemple dans l'IA ? S'agit-il de profiter d'une position dominante ?

M. Henri d'Agrain. Lorsqu'un fournisseur occupe une position dominante, il dispose de mécanismes puissants de verrouillage, communément désignés sous le terme de « *vendor lock-in* ». Ces mécanismes reposent sur plusieurs facteurs structurels. Pour une grande

organisation déjà engagée sur une solution donnée, sortir de cette solution pour migrer vers une alternative, ou même vers plusieurs alternatives, ne relève jamais d'une opération simple. Il s'agit, dans tous les cas, de projets industriels lourds et complexes.

L'exemple de la sortie de VMware est à cet égard éclairant. Pour les membres du Cigref, une telle transition implique des investissements financiers considérables, la mobilisation de compétences spécialisées, ainsi que des délais très longs. Pendant toute la durée du projet, qui peut s'étendre sur trois, quatre ou cinq ans, l'organisation ne peut évidemment pas interrompre ses services. Elle est donc contrainte de continuer à utiliser la solution initiale, de recontractualiser lorsque le contrat arrive à échéance, et d'accepter les nouvelles conditions imposées par le fournisseur.

Au terme de ce processus, l'organisation se retrouve souvent sur une solution équivalente, sans gain de productivité significatif. Elle a simplement quitté une relation devenue toxique, avec le risque d'en recréer une autre. Certaines entreprises ont ainsi envisagé de passer de VMware à Citrix, avant de constater que des mécanismes similaires de verrouillage étaient mis en place, notamment après l'arrivée, chez Citrix, d'un ancien dirigeant ayant piloté le rachat de VMware par Broadcom.

Il convient enfin de souligner que l'exploitation d'une situation de verrouillage n'est pas l'apanage des sociétés américaines. Des acteurs européens peuvent également s'inscrire dans ce type de dynamique. Ainsi, la société SAP constitue aujourd'hui un exemple régulièrement discuté avec fermeté par ses clients. Nous estimons que ces pratiques relèvent d'une exploitation abusive, même si leur qualification juridique ne nous appartient pas. C'est précisément pour cette raison que nous appelons de nos vœux des enquêtes et une intervention des autorités de régulation afin d'en apprécier objectivement la nature.

Mme Cyrielle Chatelain, rapporteure de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France. J'aimerais prolonger la réflexion que vous avez esquissée en conclusion de votre propos. Vous avez évoqué à plusieurs reprises, tant dans votre intervention introductive que dans vos réponses, ce que vous qualifiez d'« apathie » des autorités de la concurrence. Pourriez-vous préciser les freins que vous avez identifiés à l'origine de cette situation ? Existe-t-il, selon vous, un cadre juridique qui demeure inappliqué ?

Vous indiquez également ne pas avoir obtenu de retours. S'agit-il d'avis explicitement négatifs, d'échanges informels, ou d'une absence totale de réponse ? Des contacts ont-ils été noués, soit avec les autorités européennes, soit avec les autorités françaises, et si oui, avec quels résultats ? Ces éléments nous aideraient à mieux comprendre la nature de cette situation.

Par ailleurs, vous avez évoqué la régulation américaine, fondée sur la considération du numérique comme l'un des piliers de la puissance nationale. Lorsque vous suggérez d'adopter, au moins partiellement, les « lunettes » du régulateur américain, pourriez-vous nous donner des exemples concrets de dispositifs ou de pratiques que vous jugez particulièrement pertinents, même s'ils ne sauraient être transposés à l'identique dans le contexte européen ?

M. Henri d'Agrain. Votre première question est relative à l'attitude des autorités de régulation. Je demeure très prudent quant aux raisons profondes de l'apathie, voire de l'atonie, que nous constatons sur le marché B2B du numérique. Il est probable que plusieurs facteurs se conjuguent. Toutefois, certains faits objectifs méritent d'être rappelés.

Nous avons disposé d'exemples particulièrement clairs et avons, à ce titre, alerté Mme Vestager, alors vice-présidente exécutive de la Commission européenne en charge de la concurrence et, à ce titre, autorité compétente pour le contrôle des concentrations. Elle devait se prononcer sur le projet de rachat de VMware par Broadcom. Nous l'avons alertée de manière formelle et documentée, en nous appuyant notamment sur les éléments de notre saisine de 2021, en expliquant très précisément ce qui s'était produit après le rachat de CA Technologies et de Symantec Enterprise. Nous indiquions que le même scénario se reproduirait inévitablement.

Il ne s'agissait pas d'un procès d'intention, mais d'une analyse fondée sur les pratiques passées. Le PDG de Broadcom, M. Hock Tan, n'achète pas des technologies pour les faire prospérer au bénéfice de leurs clients, mais des situations de dépendance afin de les exploiter de manière intensive au service de la performance financière du groupe. C'est exactement ce qui s'est produit.

Or, engager une action contre un acteur comme Broadcom constitue une opération extrêmement complexe pour toute autorité de régulation. Cela requiert non seulement une capacité juridique élevée, mais également des instruments adaptés. Or, il me semble que les procédures actuelles du droit de la concurrence sont fondamentalement inadaptées à la dynamique temporelle des technologies numériques. Lorsqu'une autorité commence à instruire un dossier, à notifier des griefs, puis à mener une enquête approfondie qui peut durer trois, quatre ou cinq ans, le marché a déjà basculé. Les positions dominantes se sont consolidées, les modèles économiques ont évolué, et l'effet correcteur devient marginal, voire inexistant.

Nous disposons donc, selon moi, d'outils de régulation qui ne sont pas adaptés au fonctionnement du marché numérique B2B. Je ne généralise pas ce constat à l'ensemble des secteurs économiques ; il est possible que ces instruments fonctionnent dans d'autres domaines. Mais dans celui qui nous occupe, ils se révèlent manifestement inefficaces.

Une seconde raison mérite également d'être soulignée : le traitement de tels dossiers exige des compétences extrêmement spécialisées et des ressources importantes. Je ne comprends toujours pas, à titre personnel, pourquoi la saisine de 2021 n'a jamais été instruite, alors même que nos conseils juridiques nous avaient assuré de la solidité du dossier. Il est possible que les autorités aient été confrontées à un déficit de moyens, à un volume excessif de dossiers ou à la complexité particulière de ceux-ci. Je n'en ai pas la certitude, précisément parce qu'aucune explication ne nous a été fournie.

Au niveau européen, et plus spécifiquement au sein de la direction générale de la concurrence, on observe en outre une extrême prudence, sans doute liée à des considérations dépassant le strict champ du droit de la concurrence. Ces dossiers s'articulent nécessairement avec des enjeux de politique commerciale et de relations diplomatiques avec les États dont relèvent ces grands acteurs. Il n'est jamais simple de s'attaquer frontalement à des fournisseurs américains d'envergure mondiale, même lorsque les indices d'abus sont nombreux.

Du point de vue des utilisateurs européens, il existe pourtant une matière évidente à intervention, non pas en raison de la nationalité de ces entreprises, mais parce qu'elles concentrent, à elles seules, l'essentiel du marché. Sur le segment que nous observons, 83 % du marché est capté par des acteurs américains, et cette concentration obéit à la règle classique du 80-20 : environ 20 % des fournisseurs détiennent près de 80 % du marché. Nous sommes donc dans des situations de monopole ou, à tout le moins, d'oligopole.

À ce titre, l'exemple des suites collaboratives est particulièrement révélateur. Sur le marché B2B, environ 70 % des entreprises utilisent la suite collaborative Microsoft 365, près de 20 % utilisent Google Workspace, et les 10 % restants se répartissent entre une multitude d'acteurs. Dans les grandes entreprises, la réalité est encore plus tranchée.

S'agissant désormais de votre seconde question, relative à la régulation américaine, je mentionnerai deux textes fondamentaux pour comprendre la manière dont les États-Unis conçoivent la régulation du numérique. Le premier est la stratégie nationale de sécurité des États-Unis. Le second est la « stratégie cyber du Président Trump pour l'Amérique », dont le titre même est particulièrement explicite quant aux ambitions poursuivies. Ces documents expriment clairement une vision stratégique : la régulation de la technologie est indissociable de la préservation du leadership national.

Parmi les instruments concrets, je citerai le FedRamp (*Federal Risk and Authorization Management Program*), qui encadre la certification de sécurité pour l'accès aux marchés publics américains. Sans être explicitement présenté comme tel, ce dispositif produit un effet d'éviction massif à l'encontre des acteurs non américains dès lors que des enjeux de sécurité sont en jeu.

À cela s'ajoute une utilisation extrêmement volontariste de la commande publique comme levier industriel. L'histoire d'Amazon Web Services (AWS) est, à cet égard, éloquente. Avant l'attribution d'un contrat fédéral majeur de 600 millions de dollars au début des années 2010, AWS était un acteur parmi d'autres. Après ce contrat, l'activité a connu une croissance fulgurante, atteignant rapidement plus de 30 % de parts de marché mondiales, position qu'elle occupe encore aujourd'hui. En résumé, l'effet de levier de la commande publique joue un rôle majeur.

La différence essentielle avec l'Europe réside dans la rapidité des choix. Les États-Unis sélectionnent des champions, investissent de manière concentrée et agissent dans des temporalités compatibles avec le rythme du numérique. Il s'agit de procéder à de vrais choix industriels, pour ensuite grandir très rapidement.

M. le président Philippe Latombe. Je souhaiterais formuler une question complémentaire, en lien avec votre référence au règlement Dora. Sa transposition n'a pas encore eu lieu et, en France, elle est envisagée de manière articulée avec les directives NIS 2 et REC. Dès lors, pensez-vous qu'il serait pertinent d'étendre la notion de résilience, telle qu'elle est définie dans Dora, aux cadres des directives NIS 2 et de REC ? Plus précisément, la cartographie des risques exigée des acteurs devrait-elle intégrer explicitement la capacité à se défaire de dépendances technologiques identifiées comme critiques ?

Par ailleurs, les grands groupes, dont certains sont vos adhérents, ont-ils engagé ce travail ? Vous avez évoqué la protection des données les plus sensibles par des solutions « *on-premise* » ou sur site. Existe-t-il aujourd'hui, au-delà de cette approche, une réflexion structurée sur le recours à des solutions européennes ?

M. Henri d'Agrain. Notre approche ne consiste pas à appeler prioritairement à une intervention législative. Nous avons d'abord cherché à clarifier le cadre conceptuel. Nous avons repris la définition de la résilience numérique telle qu'elle est formulée dans le règlement Dora et nous avons affirmé que cette définition constituait une base pertinente pour appréhender la résilience numérique de toute grande organisation, quelle que soit sa nature.

Nous avons proposé cette définition à nos adhérents en leur indiquant qu'elle pouvait servir de référence commune. Dans le contexte actuel, où l'ensemble des grandes organisations s'interrogent sur leur résilience, et en particulier sur leur résilience numérique, cette approche rencontre un large consensus. Nous échangeons d'ailleurs depuis l'origine avec les porteurs de l'indice de résilience numérique, auxquels nous avons suggéré d'utiliser cette définition issue de Dora pour structurer leurs travaux. Il nous paraissait naturel de nous appuyer sur un texte européen existant, qui offre une définition claire et opérationnelle.

Certes, Dora n'a pas encore été transposé formellement en droit français, mais il est d'ores et déjà mis en œuvre. Les régulateurs s'en sont emparés, en particulier la Banque centrale européenne, qui supervise les banques systémiques. Depuis environ un an et demi, la dynamique est largement engagée, notamment à travers les travaux conduits avec les vingt principales banques européennes. Cette trajectoire est désormais bien enclenchée et appelée à se renforcer.

De notre côté, nous œuvrons pour diffuser cette culture de la résilience numérique auprès du public le plus large possible, en France comme en Europe. Nous avons ainsi proposé de travailler sur cette notion avec nos partenaires que sont Voice en Allemagne, CIO Platform aux Pays-Bas, Beltug en Belgique. Très récemment, l'un des vice-présidents du Cigref s'est rendu en Pologne avec un collaborateur pour échanger avec le ministre du numérique et une trentaine d'entreprises, chambres de commerce et représentants économiques, autour de cette thématique.

Il importe toutefois de préciser que la définition de la résilience numérique que nous portons ne se limite pas à la seule maîtrise des dépendances. Elle intègre également la gestion des compétences critiques, la sécurité numérique, la stratégie, la qualité des architectures et d'autres dimensions structurantes. Huit piliers, issus de Dora, permettent ainsi d'articuler l'ensemble des enjeux de la résilience numérique.

Enfin, nous ne recommandons pas d'étendre mécaniquement l'application de Dora à toutes les entreprises, ce qui serait irréaliste et difficilement applicable. En revanche, promouvoir une définition commune de la résilience numérique, partagée par le secteur public comme par le secteur privé, nous paraît constituer une démarche pertinente.

Mme Cyrielle Chatelain, rapporteure. Je souhaiterais revenir sur le chiffre des 264 milliards d'euros annuels qui irriguent l'économie américaine au titre des services numériques. Vous avez souligné à juste titre le double enjeu qui y est attaché : d'une part, une réorientation, même partielle, de ces flux vers l'Europe ; d'autre part, une diversification indispensable afin de limiter les pratiques agressives liées aux situations de quasi-monopole.

Les auditions menées convergent vers un constat clair. Cette réorientation suppose l'émergence d'acteurs européens capables d'atteindre une taille critique et de répondre aux exigences du marché. En tant que représentants de grands donneurs d'ordre, publics comme privés, vos adhérents occupent une position stratégique. Quel rôle peuvent-ils jouer dans la structuration et la montée en puissance de ces acteurs européens ? Comment peuvent-ils, par leurs choix contribuer concrètement à dynamiser un écosystème européen du numérique ?

M. Henri d'Agrain. Les grands donneurs d'ordre contribueront effectivement à l'émergence et à la consolidation d'acteurs numériques européens à la condition que l'environnement dans lequel ils évoluent soit réellement favorable. Tout l'enjeu réside précisément dans la création de cet environnement. Celui-ci suppose une mise en cohérence, au

niveau européen, de l'ensemble des instruments de politique publique – réglementation, fiscalité, commande publique et politique d'investissement. Sans cette cohérence, il est illusoire d'espérer faire émerger de véritables champions européens.

Or, aujourd'hui, dans le champ des technologies numériques, les politiques industrielles publiques souffrent d'un défaut majeur : elles refusent de faire des choix clairs. Cette indécision produit des situations que je considère, du point de vue des très grandes organisations, comme économiquement irrationnelles. Je prendrai un exemple concret : le *cloud* dit de confiance en France, tel qu'il est défini dans le cadre de SecNumCloud.

Sur ce segment stratégique, trois acteurs dits de cloud public représentent à eux seuls plus de 70 % du marché : AWS, Google Cloud et Microsoft Azure. Face à eux, sur le périmètre national, on recense une pluralité d'acteurs de cloud de confiance tels que Bleu, OVHcloud, Scaleway, Outscale, Cloud Temple, et d'autres encore. Ce sont toutes des entreprises de grande qualité, innovantes. Mais peut-on raisonnablement penser qu'une telle dispersion permettra de faire émerger un champion de taille européenne ? Pour ma part, j'ai du mal à percevoir la rationalité économique d'une telle fragmentation.

Cette question est d'autant plus sensible que les grandes entreprises, qu'elles soient publiques ou privées, opèrent à l'échelle européenne, voire mondiale. Elles ne peuvent se permettre de travailler avec un dispositif de certification en France, un autre en Allemagne, encore un autre en Espagne, et ainsi de suite. Cette hétérogénéité constitue un frein majeur à l'adoption de solutions alternatives européennes.

C'est précisément pour cette raison que nous estimons que la révision du Cyber Security Act, que l'on désigne sous le terme de CSA 2, constitue une opportunité stratégique. Elle devrait permettre de créer un schéma européen de certification de sécurité des services *cloud*, offrant des labels optionnels, adaptés aux besoins des utilisateurs. Parmi ces critères, l'intégration de garanties d'immunité à l'égard des législations extraterritoriales non européennes, lorsque cela est nécessaire, nous paraît déterminante. Un tel schéma serait un levier majeur pour accélérer le développement du *cloud* de confiance en Europe et renforcer l'émergence de véritables alternatives.

M. le président Philippe Latombe. L'absence, jusqu'à récemment, de solutions *cloud* allemandes expliquait l'opposition de l'Allemagne à certains dispositifs européens, notamment l'EUCS. Le développement de solutions de type Schwartz nous permettra-t-il de trouver une solution avec les Allemands sur le sujet ?

M. Henri d'Agrain. À mon sens, cette interprétation n'est pas la bonne. L'analyse que je propose repose sur les échanges que nous avons eus avec nos partenaires allemands. Jusqu'à la mi-2023, le schéma EUCS comprenait un niveau renforcé, dit High +, intégrant des critères d'immunité face aux législations extraterritoriales.

Le 25 mai 2023, les principales associations représentant les entreprises technologiques américaines, notamment la Computer and Communications Industry Association (CCIA) et la Business Software Alliance (BSA), ont adressé un courrier à l'administration Biden pour exprimer leur opposition à ce dispositif européen, qu'elles considéraient comme une menace potentielle pour la sécurité nationale américaine. En septembre 2023, le secrétaire d'État américain Antony Blinken a adressé une note diplomatique à la Commission et aux chancelleries européennes, indiquant que l'adoption de l'EUCS en l'état pourrait engendrer des conséquences sur les relations économiques et sécuritaires transatlantiques.

À l'automne 2023, la Commission européenne décide alors de renvoyer le schéma à l'Agence européenne de cybersécurité (Aesri). Lorsqu'il réapparaît en mars 2024, il est expurgé de l'ensemble des critères d'immunité aux législations extraterritoriales. À l'été 2024, la Commission justifie cette décision par une analyse de son service juridique, soutenant qu'un schéma de certification fondé sur le Cyber Security Act ne pourrait contenir que des critères dits « techniques », c'est-à-dire technologiques.

C'est ainsi qu'a émergé dans le CSA 2 une distinction artificielle entre risques techniques et risques non techniques, distinction qui, du point de vue des utilisateurs, n'a aucun sens. Qu'un risque soit qualifié de technique ou non, dès lors qu'il affecte la confidentialité, l'intégrité ou la disponibilité des données et des traitements associés, il constitue un risque de sécurité numérique.

En Allemagne, cette évolution s'est traduite par un revirement politique rapide. Les conséquences économiques potentielles, notamment pour l'industrie automobile très exposée au marché américain, ont pesé lourdement. Pourtant, le 30 octobre 2023, un communiqué trilatéral entre la France, l'Italie et l'Allemagne affirmait encore la volonté de travailler à un schéma européen de certification de sécurité intégrant des critères d'immunité extraterritoriale. Un mois plus tard, la position allemande avait changé.

À cela se sont ajoutées les réticences d'autres États, tels que les Pays-Bas, exprimant la crainte de restrictions d'accès au marché américain et aux garanties de sécurité américaines. Ce faisceau de pressions et de *lobbying* a finalement conduit à l'abandon des critères d'immunité dans le schéma européen de certification. Telle est, en tout cas, l'analyse que j'en fais, au regard des éléments dont nous disposons.

Mme Cyrielle Chatelain, rapporteure. Je souhaiterais revenir sur la question centrale de la réorientation des achats, en m'appuyant sur l'exemple que vous avez développé à propos du *cloud*. Nous partageons pleinement la nécessité d'une harmonisation au niveau européen et nous constatons que la France porte, sur la scène européenne, une position claire et constante en faveur de l'immunité face aux législations extraterritoriales. L'enjeu consiste désormais à convaincre nos homologues des autres États membres afin d'élargir ce consensus.

S'agissant de SecNumCloud, ma compréhension actuelle, confirmée par l'audition récente du directeur de l'Agence nationale de la sécurité des systèmes d'information (Anssi), est la suivante : en France, SecNumCloud est obligatoire pour certains types de données des administrations ou des opérateurs d'importance vitale (OIV).

M. Henri d'Agrain. Cela ne concerne que les opérateurs de l'État, et non les opérateurs d'importance vitale.

Mme Cyrielle Chatelain, rapporteure. En revanche, pour les autres entreprises, et notamment pour les grands acteurs privés, il n'existe aucune obligation de recourir à SecNumCloud. Il s'agit d'un label offrant un niveau de garanties renforcées, qui peut être intégré volontairement dans une stratégie de sécurité, mais qui ne s'impose pas juridiquement. Je tenais à clarifier ce point, car la manière dont la question avait été formulée pouvait laisser entendre une contrainte généralisée qui n'existe pas en l'état.

À l'écoute de l'ensemble des auditions, j'ai le sentiment que nous faisons face à une forme de cercle vicieux. D'un côté, de fortes attentes pèsent sur les pouvoirs publics : ils sont appelés à initier des dynamiques, à mobiliser des financements publics, à structurer des marchés

et à soutenir l'émergence d'acteurs européens. De l'autre côté, lorsque l'on interroge les acteurs privés, la réponse récurrente consiste à renvoyer la balle aux décisions publiques et à la disponibilité de financements ou de cadres réglementaires favorables.

Or ce décalage pose une difficulté majeure de politique publique. Les institutions publiques ont indéniablement un rôle déterminant à jouer : elles doivent mieux exercer leurs compétences réglementaires, utiliser la commande publique comme levier. Sur le *cloud*, par exemple, on observe des évolutions, notamment à travers la stratégie dite du « *cloud* au centre ».

Mais le risque est réel : si l'argent public et l'énergie collective mobilisés se heurtent à des verrous structurels du côté de la demande privée, nous pourrions assister à une situation où des opérateurs européens sont aidés à monter en puissance sans parvenir à trouver un marché suffisant pour consolider leur modèle économique. Certains pourraient être rachetés, d'autres disparaître faute de débouchés.

Si l'on veut véritablement créer un contrepoids aux situations de quasi-monopole actuelles et diriger une partie des flux financiers qui quittent aujourd'hui l'Europe, il faudra construire, à un moment donné, une forme de coalition entre acteurs publics et grands donneurs d'ordre privés. De quelle manière les grands acteurs privés peuvent-ils contribuer pour réorienter une partie de ces sommes ?

M. Henri d'Agrain. En tant que législateurs français, votre raisonnement repose sur un prisme essentiellement national, ce qui est compréhensible. Toutefois, la réalité des grandes entreprises internationales françaises est différente. Depuis plus de vingt ans, elles ont cherché à optimiser leurs systèmes d'information, afin de réduire les coûts et d'assurer une cohérence opérationnelle à l'échelle mondiale.

Certaines contraintes géopolitiques les ont déjà forcées à revoir cette optimisation. En Chine, elles ont dû accepter une forme de désoptimisation ou inventer d'autres équilibres. En 2022, nombre d'entre elles ont été contraintes de séparer brutalement leurs activités en Russie. Aujourd'hui, elles se retrouvent avec une organisation optimisée pour le reste du monde et commencent à s'interroger : la situation induite par les États-Unis doit-elle, à son tour, conduire à une nouvelle architecture ? À tout le moins, cette réflexion devrait pouvoir s'inscrire à une échelle européenne.

Lorsque j'évoque les conditions nécessaires, je parle de la création d'un véritable marché numérique européen. En effet, un marché fragmenté en marchés nationaux français, allemand, espagnol ou italien ne peut pas fonctionner durablement. Ce sont toujours les acteurs qui bénéficient d'un marché unifié qui s'imposent face aux autres. Pour les grandes entreprises, celles que je connais et que je représente, il est indispensable d'aboutir enfin à ce marché numérique unique, ce « *digital single market* » dont nous parlons depuis quinze ou vingt ans, sans jamais réellement le concrétiser. Il ne s'agit plus de raisonner en termes d'acteurs nationaux, mais d'identifier les grands opérateurs européens de cloud sur lesquels il conviendrait de concentrer des investissements massifs.

Si une telle dynamique voyait le jour, appuyée par des instruments comme un schéma européen de certification type EUCS garantissant une protection juridique effective des données, un consensus émergerait rapidement parmi les grandes entreprises. En revanche, désoptimiser l'organisation européenne pour multiplier des solutions fragmentées selon les pays n'est ni viable ni soutenable.

Mme Cyrielle Chatelain, rapporteure. Je souhaiterais poursuivre l'analyse afin de vérifier que nous nous comprenons pleinement. J'entends bien, et certains opérateurs *cloud* comme OVH l'ont exprimé eux-mêmes, que le marché pertinent est d'emblée européen lorsqu'il s'agit de la commercialisation des services. Le Cigref est une organisation représentant avant tout de grands donneurs d'ordre, c'est-à-dire des grandes entreprises clientes et acheteuses de solutions numériques.

Dans cette perspective, je comprends que des fournisseurs européens, qu'il s'agisse d'OVHcloud, de Scaleway ou d'autres, soulignent la difficulté de composer avec une multiplicité de normes nationales. Cela renforce l'évidence de la nécessité d'un cadre européen unifié. Par ailleurs, il semble qu'une convergence progressive soit en cours sur les exigences minimales de sécurité, ce qui permet d'espérer une meilleure cohérence à terme entre États membres.

À ce stade, votre position confirme que vous raisonnez bien prioritairement du point de vue des acheteurs. Prenons l'exemple d'une grande entreprise industrielle, active dans l'automobile ou dans un tout autre secteur sans lien direct avec le numérique. Cette entreprise n'est pas soumise aux réglementations applicables aux fournisseurs de *cloud,* son besoin est avant tout fonctionnel. Dans ce contexte, qu'est-ce qui pourrait conduire un tel acheteur à accepter une prise de risque relative en se tournant vers des acteurs européens émergents, plutôt que vers des solutions dominantes éprouvées ?

Les institutions européennes et nationales semblent déjà tester la capacité d'acteurs européens à répondre à des appels d'offres stratégiques, comme on l'a vu récemment. Si des offres commencent à émerger, la question devient alors centrale : qu'est-ce qui ferait basculer un grand acheteur privé ? Si des solutions existent ou sont en voie d'exister, quels leviers concrets permettraient aux acheteurs privés de franchir le pas et de contribuer, par leurs choix, à la construction d'un écosystème numérique ?

M. Henri d'Agrain. En effet, le Cigref représente des grandes organisations qui achètent, mais elles conçoivent également leurs architectures de systèmes d'information, administrent leurs infrastructures et, dans de nombreux cas, développent elles-mêmes une part significative des services numériques qu'elles utilisent. Réduire une direction du numérique ou des systèmes d'information à un simple service achat constituerait une méconnaissance profonde de sa réalité et de ses responsabilités, quels que soient les secteurs d'activité concernés.

Dans certaines industries, et notamment dans le secteur bancaire, l'outil de production est avant tout numérique. Un réseau ferroviaire européen ne peut fonctionner efficacement si chaque pays adopte un écartement de rails différent. Dans ce cas, le train devient inutilisable au profit du transport routier, avec toutes les externalités négatives que cela implique, notamment en termes d'émission de CO_2.

C'est exactement la situation à laquelle nous sommes confrontés dans le numérique européen. Les grandes organisations doivent opérer à l'échelle du continent. Si les normes, cadres et architectures diffèrent d'un État à l'autre, elles renoncent à ces solutions fragmentées et se tournent vers des plateformes globales, unifiées, principalement américaines. Autrement dit, l'absence d'un socle européen cohérent conduit mécaniquement les acteurs à privilégier des solutions extérieures, par nécessité opérationnelle.

Mme Cyrielle Chatelain, rapporteure. Permettez-moi de préciser ma question. Une fois qu'une grande entreprise a structuré en interne ses architectures et identifié les besoins qu'elle ne peut satisfaire seule, est-elle aujourd'hui en mesure de trouver des offres françaises ou européennes capables de prendre en charge cette complexité ?

Ma seconde interrogation demeure inchangée depuis le début de nos échanges. Quelle part les grands acheteurs peuvent-ils prendre, d'autant plus qu'ils disposent souvent de fortes compétences internes, dans la dynamique visant à accompagner et à renforcer l'émergence d'opérateurs européens ?

M. Henri d'Agrain. Je choisirai résolument une posture optimiste. La conscience est désormais largement partagée : il est impératif de renforcer la résilience de l'économie européenne. Cette prise de conscience se traduit par des réflexions engagées au sein de nombreux acteurs. Lors du Forum international de la cybersécurité l'an dernier, M. Patrick Pouyanné lui-même soulignait que, lorsqu'un opérateur n'a le choix qu'entre trois acteurs américains, une forme de malaise s'installe, y compris pour une entreprise dont l'activité est très largement implantée aux États-Unis.

La réalité est aujourd'hui la suivante : pour opérer efficacement à l'échelle mondiale – et, *a minima*, à l'échelle européenne –, peu d'acteurs sont en mesure d'offrir les performances, l'étendue fonctionnelle et la maturité technologique des *hyperscalers* américains. Nous pouvons toutefois espérer une réduction progressive de cet écart. Des acteurs européens comme OVHcloud, Scaleway ou encore Stackit au sein du groupe Schwarz, commencent à proposer des services à l'échelle. Néanmoins, force est de constater qu'ils ne disposent pas encore de la même richesse fonctionnelle que leurs homologues américains.

Cela étant, la prise de conscience progresse rapidement. De plus en plus d'adhérents nous interrogent sur les alternatives existantes, sur les trajectoires possibles et sur les stratégies de diversification. L'élément déterminant, toutefois, demeure la création des conditions d'environnement permettant d'accélérer concrètement ces choix. En l'absence de cohérence entre les différentes politiques publiques – européennes ou nationales – les évolutions resteront marginales. Même dans le secteur public, malgré certaines inflexions positives, les mécanismes actuels ne suffisent pas à provoquer un véritable effet de marché.

Prenons un exemple précis : la commande publique numérique. Pour produire un effet structurant, elle doit être massifiée. Or, l'autonomie de gestion des collectivités territoriales empêche aujourd'hui d'activer pleinement ce levier à l'échelle nationale et européenne, tant pour le *cloud* que pour le logiciel. Il en résulte un financement dispersé d'une multitude d'acteurs, aussi compétents soient-ils, mais qui contribue *in fine* à maintenir le *statu quo* plutôt qu'à faire émerger de véritables champions européens.

Mme Cyrielle Chatelain, rapporteure. Plusieurs interrogations surgissent autour de ce chiffre désormais central des 264 milliards d'euros. La première concerne la répartition entre achats publics et achats privés.

M. Henri d'Agrain. Je ne saurais vous dire, à l'échelle européenne, l'exercice est complexe. Si je prends le périmètre du Cigref, on estime à près de 100 milliards d'euros par an les achats informatiques, tous périmètres confondus, à l'échelle mondiale. À titre d'illustration, quatre banques systémiques concentrent à elles seules environ un cinquième de ce montant, soit un peu plus de 20 milliards d'euros. À titre de comparaison, les achats de l'État représentent un peu plus de 4 milliards d'euros par an. Cela signifie que la commande publique étatique *stricto sensu* correspond à 4 % à 5 % du total. Ce chiffre suffit à montrer que le levier public, pris isolément, demeure relativement limité.

Mme Cyrielle Chatelain, rapporteure. Cela renvoie précisément à la question du levier privé. C'est précisément à ce stade qu'apparaît une difficulté plus profonde, commune aux acteurs privés comme aux acteurs publics, c'est-à-dire une forme de verrouillage culturel. Comme pour l'utilisateur particulier, les organisations se sont habituées à certains services, à des usages, y compris pour des fonctionnalités qu'elles n'utilisent pas nécessairement, mais qu'elles savent disponibles. Comment amorcer un changement culturel permettant d'accepter que la transition ne se fasse jamais à l'identique ?

Par ailleurs, l'Anssi nous indiquait que des investissements importants avaient été effectués. Réorienter les choix suppose nécessairement des coûts – coûts financiers, coûts organisationnels – puisque sortir d'une solution implique souvent de faire fonctionner des systèmes en parallèle et de réinvestir.

Dès lors, percevez-vous aujourd'hui une réelle disposition des acteurs économiques à consentir cet effort, au moins partiellement ?

M. Henri d'Agrain. Une entreprise ne décidera jamais de quitter une solution existante et d'engager des efforts significatifs si cette démarche n'apporte aucun bénéfice tangible. Elle ne le fait que si cela répond à un besoin directement lié à son activité, à sa productivité, à sa compétitivité. En l'absence d'enjeu avéré, notamment en matière de sécurité, les entreprises n'ont aucun rationnel économique pour changer.

J'en discutais récemment avec la dirigeante d'un grand adhérent du Cigref, une entreprise française dont plus de 50 % de l'activité est réalisée aux États-Unis, y compris à travers des marchés publics conclus avec des agences fédérales américaines. Dans une telle configuration, le recours à Microsoft s'impose de fait ; ne pas l'utiliser reviendrait à se priver d'une part essentielle de son marché. Lorsqu'une entreprise réalise la moitié de son chiffre d'affaires aux États-Unis, il n'existe aucun raisonnement économique consistant à se dire qu'en France elle adopterait une solution, par exemple *open source*. Les situations sont donc extrêmement hétérogènes selon les modèles d'affaires et les géographies.

Il faut également dépasser l'idée selon laquelle ces arbitrages relèveraient uniquement d'un problème de culture. Bien sûr, la culture de la sécurité et de la résilience est essentielle, et les entreprises ont accompli un travail considérable sur ces sujets ces dernières années : sur la cybersécurité, sur la protection de leur patrimoine informationnel, et désormais sur la résilience globale de leurs systèmes. Mais cette évolution culturelle ne conduit pas mécaniquement à des choix industriels si ceux-ci ne génèrent pas une plus-value en termes de résilience, de renforcement de la sécurité, d'impact positif sur leur productivité et leur compétitivité.

C'est dans cette logique que s'inscrit aujourd'hui la dynamique à l'œuvre au sein de ces entreprises : l'hybridation des systèmes d'information. Cette hybridation consiste à recourir à plusieurs fournisseurs, sur différentes zones géographiques et pour des briques spécifiques de la chaîne technologique. Elle complexifie l'exploitation des systèmes, nécessite des compétences multiples et renchérit les coûts opérationnels. Lorsqu'une entreprise opère avec un seul fournisseur *cloud*, elle forme ses équipes sur cet environnement. En en mobilisant deux pour des fonctions similaires, elle doit doubler ses compétences, donc ses efforts de formation et ses dépenses.

À cela s'ajoute une contrainte forte, qui correspond à la disponibilité des compétences sur le marché. Les grandes entreprises du numérique forment massivement aux technologies d'AWS, d'Azure ou de Google Cloud. Les compétences existent beaucoup moins pour exploiter des plateformes européennes, même si, sur le plan technique, les différences ne sont pas fondamentales.

M. le président Philippe Latombe. Quelles seraient aujourd'hui vos préconisations pour éviter de reproduire les mêmes erreurs, dans le financement des entreprises innovantes et dans l'achat de produits IA ?

M. Henri d'Agrain. À titre personnel, et au regard des évolutions actuelles dans le domaine de l'intelligence artificielle, je souhaite partager une conviction. Nous nous trouvons, selon moi, à un moment d'urgence stratégique pour l'Europe, comparable à des ruptures historiques telles que la crise de Suez en 1956 ou le choc pétrolier de 1973. Ces événements avaient conduit la France, sous l'impulsion du général de Gaulle puis du plan Messmer, à faire des choix décisifs en matière d'autonomie stratégique, notamment dans les domaines nucléaire et énergétique. La situation géopolitique actuelle, appliquée au numérique et à l'intelligence artificielle, appelle une réflexion de même nature à l'échelle européenne.

Il serait pertinent d'envisager la création d'une structure européenne de référence, qui jouerait un rôle comparable à celui du Commissariat à l'énergie atomique (CEA) à ses débuts, c'est-à-dire une entité capable d'éclairer l'avenir par la recherche fondamentale et appliquée, et de soutenir massivement l'innovation par l'investissement.

Dans le champ de l'intelligence artificielle, les dynamiques temporelles sont infiniment plus rapides et exigent des réponses à la hauteur. Cela suppose d'assumer des choix clairs : sélectionner un nombre limité d'acteurs européens et les soutenir de manière déterminée afin de bâtir une autonomie stratégique indispensable. Les compétences existent, les bases technologiques et scientifiques sont bien présentes en Europe. Ce qui fait aujourd'hui défaut, c'est une volonté politique forte, inscrite dans la durée et capable de résister aux fluctuations conjoncturelles.

Sans un tel engagement, des dépendances systémiques risquent de s'installer durablement et de se renforcer. L'enjeu consiste donc à financer rapidement les infrastructures critiques, de soutenir les équipes de recherche et de définir une stratégie cohérente, portée par une détermination politique constante

M. le président Philippe Latombe. Je vous remercie. N'hésitez pas à nous adresser des contributions écrites, afin de compléter vos propos.

La séance s'achève à douze heures vingt.

———

Membres présents ou excusés

Présents. – Mme Cyrielle Chatelain, M. Philippe Latombe