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

Mardi
21 avril 2026
Séance de 14 heures

Compte rendu n° 31

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à quatorze heures.

La commission entend, lors de sa table ronde réunissant des fournisseurs de cloud :

– M. Eric Haddad, président exécutif de NumSpot,

– M. Octave Klaba, président-directeur général d'OVHcloud, et Mme Solange Viegas Dos Reis, directrice juridique,

– M. Sébastien Lescop, directeur général de Cloud Temple,

– M. Damien Lucas, directeur général de Scaleway

– M. Philippe Miltin, directeur général d'Outscale Dassault Systèmes, et M. David Chassan, directeur de la stratégie.

M. le président Philippe Latombe. Nous réunissons cet après-midi, pour une table ronde, les fournisseurs français de cloud, à qui je laisserai la parole pour un propos liminaire d'environ cinq minutes chacun. Je vous demanderai de nous présenter succinctement votre activité et de nous indiquer comment vous vous positionnez par rapport à la forte croissance de la demande de cloud dans le secteur public. La demande publique amorce-t-elle celle du secteur privé ? La norme SecNumCloud est-elle pertinente ? Toutes ces questions sont intéressantes pour nous aujourd'hui. Je vous demanderai d'être brefs, sans que cela doive obérer l'exhaustivité de vos propos, mais comme nous sommes relativement nombreux, l'idée est de pouvoir ensuite échanger sous forme de questions-réponses.

Je vous remercie de nous déclarer au préalable tout intérêt public ou privé de nature à influencer votre déclaration. 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, rien que la vérité.

(*Mme Solange Viegas Dos Reis et MM. Sébastien Lescop, Éric Haddad, Philippe Miltin, David Chassan, Octave Klaba et Damien Lucas prêtent serment)*.

M. Sébastien Lescop, directeur général de Cloud Temple. Je voudrais d'abord remercier cette commission pour l'enquête qu'elle conduit. Elle va dans le sens d'un combat que nous menons au quotidien avec nos confrères ici présents : en finir avec l'idée reçue que la sécurité et la souveraineté seraient incompatibles avec la performance. C'est faux, et nous en sommes la démonstration quotidienne.

La France a construit des secteurs industriels d'une puissance rare : le nucléaire, l'aéronautique, la pharmacie, la banque ; des secteurs qui font que la France pèse dans le monde économiquement, diplomatiquement et stratégiquement. Ces secteurs se numérisent à une vitesse que nous n'avions pas anticipée. C'est une transformation souhaitable, mais à une condition : que nous en conservions la maîtrise. Or, nous sommes en train de la perdre, non par négligence, mais par défaut de choix industriels assumés. La part des acteurs européens dans le cloud est passée de 27 % en 2017 à 15 % aujourd'hui. 265 milliards d'euros de dépenses numériques européennes partent chaque année vers des entreprises étrangères. La tech

représente 10 % du PIB en Chine et aux États-Unis, et seulement 5 % en France et en Europe. Ce n'est pas un problème de talent ici, c'est un problème de choix industriels.

Pendant longtemps, la dépendance technologique était un problème que l'on pouvait circonscrire. On achetait à l'étranger des composants, des logiciels, et on conservait ici la compétence, la décision, la valeur. La technologie traitait des données, la connaissance restait chez nous. Ce n'était déjà pas sans risques : des données de santé hébergées hors juridiction, des secrets industriels confiés à des infrastructures étrangères, des processus stratégiques dépendants d'acteurs soumis à des lois extraterritoriales. La vulnérabilité était réelle, même si elle restait contenue.

L'intelligence artificielle franchit un seuil supplémentaire. Pour la première fois, la technologie ne traite plus seulement des données, elle traite de la connaissance. Elle assiste à la décision médicale, juridique, financière, stratégique. Ce n'est plus l'accès aux données qui est en jeu, c'est l'accès au raisonnement, à l'analyse, à la décision elle-même.

Il n'y aura pas d'intelligence artificielle souveraine sans cloud de confiance. Héberger des modèles d'IA sur des infrastructures que l'on ne contrôle pas, c'est externaliser simultanément nos données et notre capacité d'innovation. Quand un hôpital confie ses protocoles à une IA non souveraine, quand un laboratoire pharmaceutique fait tourner ses simulations hors de notre juridiction, quand un groupe industriel optimise ses processus critiques sur une infrastructure qu'il ne contrôle pas, ce n'est plus une question de confidentialité ni de risque de cybersécurité : c'est un risque de désindustrialisation cognitive.

La souveraineté numérique est souvent représentée comme un bouclier. Je vous propose de la penser comme une stratégie de puissance, offensive et non défensive. 70 % des infrastructures mondiales ne sont pas encore dans le cloud. La partie se joue maintenant. C'est probablement la plus grande opportunité industrielle de la décennie pour les acteurs européens. Il existe un baromètre simple pour évaluer toute décision de politique numérique : cette décision crée-t-elle de la puissance technologique ici, des emplois qualifiés sur notre territoire, une industrie qui irrigue nos secteurs stratégiques plutôt que de les fragiliser ? Chaque décision d'achat qui choisit un acteur dont la chaîne de valeur garantit l'indépendance est un acte industriel. Elle crée de la puissance, des emplois et de l'industrie sur notre territoire.

Cloud Temple est né d'une conviction : certaines infrastructures numériques doivent rester sous contrôle européen, avec la plus haute exigence de sécurité. Comme les budgets de cybersécurité n'avancent jamais aussi vite que la menace, la seule réponse viable dans le temps est une sécurité construite à l'échelle industrielle et intégrée dès la conception. Nous sommes un *pure player* de la sécurité sur le marché du cloud français. L'intégralité de notre catalogue est qualifiée SecNumCloud ou ambitionne de le devenir. Nous finalisons actuellement la qualification Prestataire d'administration et de maintenance sécurisées (Pams), un autre référentiel de l'Agence nationale de la sécurité des systèmes d'information (Anssi) pour les cas d'usage que SecNumCloud ne couvre pas. Nous portons cette exigence à l'échelle européenne en passant les certifications équivalentes en Allemagne, en Italie et en Espagne.

Nos clients couvrent les secteurs qui ne peuvent pas se permettre de faillir : la défense, l'industrie, la finance, la santé. Parmi eux figurent la direction générale de l'armement (DGA), Naval Group, Framatome, la Banque de France, EDF, Veolia ou encore le Samu. Pour eux, la sécurité est non négociable. Nous sommes la preuve que des alternatives sont possibles.

M. Éric Haddad, président exécutif de NumSpot. NumSpot a été créée en 2023 pour répondre précisément au sujet qui nous réunit aujourd'hui. L'entreprise a été fondée à l'initiative de la Banque des territoires, donc de la Caisse des dépôts, de Docaposte, de Dassault Systèmes et de Bouygues Telecom. L'idée de départ était d'offrir aux administrations et, d'une façon générale, aux métiers régulés qui gèrent des données sensibles, une alternative aux clouds américains et chinois. Nous sommes aujourd'hui une entreprise à dominante technologique, majoritairement composée d'ingénieurs, avec une proportion de femmes en augmentation.

Nous nous sommes aperçus assez rapidement qu'ajouter une offre verticale supplémentaire de cloud français risquait d'être dilutif par rapport au marché et à sa taille. Nous avons donc décidé de nous positionner davantage comme une plateforme inclusive de l'écosystème. C'est ainsi que nous avançons et que nous faisons évoluer notre feuille de route. L'idée est d'apporter un haut niveau de souveraineté grâce à la conformité de nos services. Certains référentiels ont été cités : bien entendu ISO 27001, hébergeur de données de santé (HDS) pour les données de santé, SecNumCloud, et nous regardons avec beaucoup d'attention tout ce qui se passe au niveau européen.

Nous le faisons avec un haut niveau d'autonomie et de capacité de réversibilité pour nos clients et les institutions qui nous font confiance, grâce à une approche 100 % open source. Tout ce que nous produisons est en open source ; nous n'utilisons aucune licence dans le développement et la construction de nos logiciels. Nous le faisons avec une indépendance opérationnelle, liée au fait que nous n'avons ni filiale ni organisation extra-européenne. Tout cela est développé en cohérence avec l'un de nos actionnaires, Dassault Systèmes, puisque nous développons notre plateforme sur l'infrastructure d'Outscale. Toutefois, de manière logique et cohérente avec une approche inclusive de l'écosystème, nous faisons en sorte que notre plateforme soit portable sur d'autres types d'infrastructures. Cela nous permettrait une expansion européenne en nous appuyant sur les infrastructures locales de nos pays voisins.

Nous le faisons aussi en anticipant les besoins en processeurs spécialisés pour l'IA, qui sont extrêmement rares aujourd'hui, afin de pouvoir nous déployer sur des infrastructures spécialisées, je parle en l'occurrence de clusters de GPU, si vous connaissez ce terme. Nous répondons également aux besoins des entreprises et des administrations qui ont beaucoup investi dans des clouds privés internes et qui ont des besoins d'hybridation entre leurs infrastructures internes et la capacité de déborder de façon élastique et agile sur des clouds publics. C'est ce que peut apporter la plateforme NumSpot.

L'ensemble de nos actionnaires, de nos ingénieurs et de nos partenaires rejoint ce projet, car nous avons une conviction, qui relève presque de la foi, quant à cette nécessité de souveraineté que Sébastien Lescop a largement présentée et que mes successeurs, j'en suis sûr, aborderont également. Le message est le suivant : serons-nous suivis ? Les pouvoirs publics qui nous accompagnent et nous supportent pourront-ils aider à l'accélération de ce marché qui, objectivement, au vu du nombre d'acteurs présents, est aujourd'hui relativement petit au niveau national et européen ?

M. Philippe Miltin, directeur général d'Outscale Dassault Systèmes. Outscale est une marque de Dassault Systèmes, créateur de valeur industrielle au service de 400 000 clients de toute taille et de tout secteur dans 159 pays. Le groupe a enregistré l'année dernière un chiffre d'affaires de plus de 6 milliards d'euros et se positionne comme le premier éditeur de logiciels français. Dassault Systèmes regroupe treize marques, parmi lesquelles Outscale, qui opère la plateforme cloud et IA du groupe pour l'ensemble de ses clients.

Notre mission, depuis 2010, est de démontrer qu'une souveraineté numérique effective est possible et réelle. Nous avons répondu aux exigences les plus strictes : premier cloud français intégralement certifié ISO 27001, certifié HDS, Tisax (*trusted information security assessment exchange*) et, enfin, premier cloud public qualifié SecNumCloud depuis 2019. Aussi, nous travaillons avec les sociétés les plus performantes et exigeantes au niveau mondial sur des cas d'usage sensibles, en leur proposant à la fois des services de cloud et d'IA. Outscale a donc la singularité de fournir des services de cloud et d'IA à l'échelle mondiale pour Dassault Systèmes et ses 400 000 clients, d'élargir sa proposition de service auprès du secteur public, des acteurs de la santé et de la finance, et de développer des services d'IA souveraine et d'IA industrielle connectés à la science.

Le sujet de votre commission d'enquête est l'un des plus stratégiques pour la France et l'Europe. C'est également une préoccupation mondiale. Le marché mondial du cloud est structurellement déséquilibré : trois acteurs américains, AWS, Microsoft Azure et Google Cloud, représentent plus des deux tiers du marché global. En France, les acteurs européens et français ont capté une part croissante de la commande publique. Le marché du cloud public affiche une hausse de 62 %, mais la réalité de l'ensemble du marché privé reste largement gouvernée par les *hyperscalers*. Cette situation expose à des risques qui renvoient à trois dépendances : juridique, opérationnelle et technologique.

La dépendance juridique désigne la capacité d'une autorité étrangère à s'appuyer sur ses lois à portée extraterritoriale pour obliger un acteur du cloud soumis à ce droit de lui remettre des données, même sans l'autorisation des autorités ou du client concerné. Nous parlons communément des États-Unis, mais la Chine, l'Inde, le Canada, le Brésil et l'Australie sont tous des exemples de pays qui intègrent dans leur droit des lois à portée extraterritoriale.

La dépendance opérationnelle désigne l'absence de maîtrise sur les opérations, les accès et les personnels qui administrent l'infrastructure. Elle se caractérise par une exploitation confiée à des équipes hors de la juridiction locale, sans auditabilité vérifiable, sans gestion des identités et des accès sous le contrôle du client, et sans modèle de gouvernance cyber adapté aux exigences de l'organisation. Cette opacité devient critique dans les situations de crise ou de contrôle réglementaire.

Enfin, la dépendance technologique désigne l'enfermement progressif dans des choix techniques propriétaires : piles logicielles en boîte noire, formats et API non interopérables. Plus une organisation construit ses services sur ces briques, plus le coût de migration augmente et plus la capacité à changer de fournisseur se réduit. Cette dépendance expose au risque d'indisponibilité et entraîne mécaniquement une perte de résilience. Tolérer l'installation de ces dépendances revient à s'exposer à des risques accrus en matière de protection des données et de la propriété intellectuelle, de hausse des coûts et de continuité de service, autant de vulnérabilités qui peuvent servir de leviers de pression et d'affaiblissement de notre position sur la scène internationale.

En réponse à cela, depuis sa création, Outscale a construit une architecture qui adresse simultanément ces trois dimensions de la dépendance. Nous fondons notre approche sur trois piliers indissociables, qui sont la traduction de la lutte contre ces dépendances. L'autonomie juridictionnelle : Outscale est une entité française, marque de Dassault Systèmes, société cotée française. Notre structure capitalistique et organisationnelle nous place hors du champ d'application des lois à portée extraterritoriale. L'autonomie opérationnelle : nos équipes, nos processus, notre gouvernance et notre support sont entièrement situés en France et en Europe. L'indépendance technologique et financière : notre système d'orchestration de cloud, Tina OS,

est développé en interne à base de briques open source. Il introduit une couche de virtualisation. Notre pile logicielle critique repose sur des technologies que nous maîtrisons et qui permettent l'interopérabilité et la réversibilité. Nous disposons de notre propre capacité d'investissement, ce qui nous permet d'assurer nos propres choix sans ingérence.

Une garantie nous distingue fondamentalement des *hyperscalers* : nous ne facturons aucuns frais de sortie. Un client qui souhaite partir le fait sans pénalité technique ni financière. C'est ce que nous entendons par une réversibilité réelle, et c'est une position largement partagée au sein de l'écosystème du cloud français et européen.

Alors, où en sommes-nous ? Des progrès réels ont été accomplis et des actions sont à renforcer. Chez Outscale, nous défendons une stratégie de la complémentarité, du « et » plutôt que du « ou » : confier les données sensibles et les traitements critiques à des offres souveraines, sans s'interdire de recourir aux *hyperscalers* ou à d'autres clouds de communauté pour des usages moins sensibles. L'essentiel pour l'acheteur est d'être au clair sur les dépendances auxquelles il s'expose et de les choisir en connaissance de cause. Il nous semble que cette prise de conscience est encore insuffisante et qu'il est possible de progresser vers plus de pédagogie sur les garanties proposées par chaque type d'offre. En témoigne le débat autour de SecNumCloud lorsque la première offre hybride a été qualifiée, qui déplace désormais les enjeux de résilience vers les questions de dépendance technologique et de capacité à se protéger contre un risque de rupture de service.

La stratégie cloud de l'État, et notamment la doctrine « cloud au centre », a produit des effets positifs. Nous reconnaissons qu'elle a joué un rôle important dans l'orientation de l'achat public vers des offres de marché souveraines. Les annonces publiques récentes en faveur d'une commande publique mieux ciblée sont également positives. Nous ne pouvons qu'encourager le renforcement des supports de sensibilisation et d'accompagnement des acheteurs publics de cloud sur les enjeux de souveraineté numérique. Le lancement, le 8 avril dernier, du plan interministériel de réduction des dépendances extra-européennes, qui prévoit l'élaboration par chaque ministère d'une stratégie de réduction de ses dépendances numériques, peut également servir de levier structurant. Mais nous remarquons que certaines grandes économies mondiales ne se gênent pas pour soutenir directement leurs champions technologiques. Nous devons faire la même chose en France et en Europe, via une préférence assumée pour la technologie, en particulier sur les usages sensibles.

Nous soutenons également que des progrès peuvent être faits dans la manière dont les centrales d'achat présentent et catégorisent les offres souveraines. Les modes de présentation actuels ne permettent pas aux acheteurs publics d'identifier rapidement quelles solutions offrent des garanties sérieuses de souveraineté et quelles offres les exposent à des risques de dépendance. Plus encore, cette confusion ne permet pas aux entités publiques soumises aux obligations de la loi Sren de distinguer clairement quels fournisseurs de cloud leur permettent de se mettre en conformité. Les offres de cloud SecNumCloud pourraient être rassemblées et mises en avant dans des catégories dédiées des catalogues et sites des centrales d'achat.

La réduction des dépendances numériques, tout particulièrement pour les services de cloud, est une condition de notre autonomie stratégique. Les solutions existent, elles sont matures et déjà disponibles en France et en Europe. D'ailleurs, le niveau européen est sans doute le plus pertinent pour traiter cette problématique, car il offre assez de profondeur de marché pour permettre aux solutions souveraines d'atteindre une taille critique. La France et son écosystème ont été particulièrement moteurs sur ces questions de souveraineté, de protection des données sensibles, de résilience technologique et de réduction des dépendances.

Les grands rendez-vous européens à venir, comme la révision du Cyber Resilience Act et l'adoption du règlement Cada sur le cloud souverain, seront déterminants. Nous formons donc le vœu que les ambitions de votre commission d'enquête puissent être aussi concrétisées au niveau européen. L'enjeu est aussi d'ordre politique : il s'agit de développer les conditions d'un choix éclairé et pleinement assumé. Outscale, aux côtés de l'écosystème, est prêt à y contribuer.

M. Octave Klaba, président-directeur général d'OVHcloud. Cela fait vingt-huit ans que je fais ce métier. J'ai créé l'entreprise en 1999 avec cette idée d'indépendance, probablement pour des raisons que l'on pourrait qualifier de paranoïaques au début, mais qui se sont avérées très positives par la suite. Très tôt, nous avons investi dans nos propres data centers. Très tôt, nous avons investi dans nos lignes de production de serveurs. L'ensemble de l'infrastructure que nous déployons dans les data centers provient de nos usines de fabrication, dans lesquelles nous choisissons, testons et validons l'ensemble des composants que nous utilisons. Côté logiciel, nous avons progressivement ajouté différentes couches que nous appelons aujourd'hui public cloud, *private* cloud et d'autres typologies de cloud. L'entreprise a évolué avec cette volonté et cette nécessité d'indépendance pour éviter d'être bloquée dans son déploiement et son expansion. Telle était la motivation initiale. À travers l'open source et le développement de produits, nous avons décidé d'investir dans des couches supplémentaires à partir de 2010 environ, en apportant des services de cloud additionnels à nos clients. Nous nous sommes étendus dans de nombreux pays, en Europe et à travers le monde.

Qu'avons-nous cherché à travers cela ? Une certaine masse critique. Les investissements sont si importants qu'on ne peut compter sur un seul pays ou un seul secteur vertical pour les rentabiliser. Il faut donc chercher une masse critique à travers le nombre de clients, de pays, de stratégies de commercialisation et les différentes typologies de clients – consommateurs, professionnels, grandes entreprises, secteur public – pour pouvoir assumer ces investissements.

Aujourd'hui, la commande publique a évolué positivement, surtout ces trois dernières années, grâce notamment à SecNumCloud. Mais on parle de millions d'euros. C'est très bien, c'est déjà mieux qu'il y a cinq ou dix ans, où l'on n'en parlait pas. Mais pour atteindre une taille critique, il faut parler en milliards. Et aujourd'hui, cette échelle, on ne l'entend pas en Europe. Nous l'avons vue ces dix ou quinze dernières années aux États-Unis, où la commande publique a sponsorisé le développement de technologies auprès des *hyperscalers*, grâce à des contrats de plusieurs dizaines de milliards de dollars, ce qui leur a permis de créer les offres que l'Europe attendait. Aujourd'hui, la commande européenne se chiffre en millions ou en dizaines de millions, pas en milliards. D'ailleurs, en Europe, il n'existe pas de contrats de plusieurs dizaines ou centaines de millions d'euros ; ce sont des ruisseaux d'affaires de 100 000 euros à un million par an.

La difficulté que nous avons en Europe pour construire des géants est que nous avons de nombreux pays, langues et devises. La complexité pour toucher ces marchés et générer suffisamment de revenus à réinvestir est immense, car tout est extrêmement segmenté et subdivisé. Il faut être présent presque partout, avec des coûts que n'a pas un acteur américain. Aux États-Unis, il suffit d'être présent sur la côte Est et la côte Ouest pour avoir l'ensemble du pays à sa portée, en parlant anglais et en faisant des affaires en dollars. Ce sont principalement ces freins structurels que nous avons en Europe. Je n'ai pas de solution à ces problèmes, si ce n'est peut-être un courage et une volonté de la part des institutions et du secteur privé.

Aujourd'hui, nous existons en réalisant 1,2 milliard d'euros de chiffre d'affaires, ce qui est peu. Dans le cloud, 1,2 milliard de chiffre d'affaires reste modeste, car cela ne permet

d'investir que 350 millions par an. Mais nous avons atteint une taille qui nous permet d'envisager de nouveaux développements et de continuer notre croissance. Nous nous situons dans un moment assez opportun, car l'administration américaine montre des intentions qui, en tant qu'Européens, nous effraient. Forcément, cela contribue à rendre concrets les concepts de souveraineté et de dépendance dont nous parlons depuis une dizaine d'années, comme en témoigne cette commission. Des événements comme le rachat de VMWare par Broadcom constituent une autre onde de choc qui a rendu très nerveux l'ensemble des acteurs du numérique en Europe, notamment les clients.

Nous sommes donc dans un moment opportun, car cette discussion est enfin sur la table. Maintenant, il faut la transformer pour créer des géants capables de réaliser 5, 10 ou 20 milliards de chiffre d'affaires. Est-ce possible ? Prenez juste cet exemple, qui est une estimation : si vous prenez le secteur public en Europe – l'ensemble des gouvernements et la Commission européenne –, vous avez environ 10 milliards d'euros de chiffre d'affaires annuel qui partent chez AWS, Azure et Google, et très peu chez les acteurs européens. La Commission européenne a bougé et a lancé un appel d'offres de 180 millions d'euros, attribué à quatre acteurs. C'est un excellent démarrage. Je pense que nous devrions voir davantage ce genre d'initiatives en Europe, car c'est précisément ainsi que nous créerons la masse critique nécessaire pour permettre à ces entreprises d'évoluer et d'investir.

Je suis plein d'espoir. Il a fallu plus de vingt ans d'attente, mais ce moment est enfin arrivé. Nous croyons qu'il est possible de faire des choses, et c'est encore plus important. Nous sommes portés par l'ensemble des acteurs du marché, pas seulement de notre côté. Les clients, les acteurs financiers, tous croient qu'il est possible aujourd'hui de créer, et nous avons une vraie volonté de le faire.

M. Damien Lucas, directeur général de Scaleway. Scaleway est une filiale du groupe Iliad. C'est un point important, car le directeur général du groupe, Thomas Reynaud, a annoncé il y a quelque temps un investissement de 4 milliards d'euros dans le cloud et l'IA. Quatre milliards, c'est l'ordre de grandeur des investissements dont nous avons besoin, et j'y reviendrai.

Chez Scaleway, nous faisons du cloud public. Le cloud public, ce n'est pas seulement héberger des serveurs, c'est fournir une boîte à outils à nos clients. Évidemment, plus cette boîte à outils est complète, plus nos clients seront efficaces pour construire leurs applications. Nous sommes également un cloud « boosté à l'IA », avec la plus grande capacité de calcul dédiée à l'IA dans le cloud en Europe aujourd'hui. C'est important pour l'avenir. Les perspectives de l'entreprise sont bonnes, voire très bonnes. Nous accroissons nos effectifs de plus de 100 personnes chaque année et notre croissance est probablement trois fois supérieure à celle du marché.

Notre proposition de valeur est double, et je ne parlerai pas de souveraineté, car on ne sait plus très bien ce que l'on met sous ce label, qui a peut-être été victime d'un peu trop de « sovereignty washing ». Je parlerai de deux choses. Premièrement, l'immunité aux lois extraterritoriales. Comme ces lois étrangères évoluent, chez Scaleway, nous appliquons un concept très simple : pas d'actionnaire direct ou indirect en dehors de l'Europe, pas de filiale en dehors de l'Europe et pas de personnel en dehors de l'Europe. Cela permet de garantir à nos clients que leurs données seront protégées contre l'ingérence de puissances extérieures. La deuxième proposition de valeur est l'indépendance technologique. Nous développons tous nos logiciels. Nous utilisons évidemment de l'open source, mais nous ne dépendons d'aucune licence tierce, que ce soit de VMWare, Broadcom, IBM, Red Hat, Microsoft ou Google.

Pourquoi est-ce important ? Pour éviter le risque de *kill switch*. Trop souvent, on réduit le cloud à la question de la protection de la donnée. Mais il est encore plus important de protéger les flux de travail et les opérations de nos clients. Nous le savons, quand il y a une panne chez Azure ou AWS, les avions européens sont cloués au sol. Si l'on coupe le cloud, plus rien ne fonctionne dans notre économie. Oui, il faut protéger la donnée, mais il faut également se protéger contre l'arrêt intempestif du cloud.

Pour vous donner quelques ordres de grandeur, les investissements sont très importants : un euro de croissance, ce sont trois euros d'investissement. On parlait de corriger la part de marché en milliards ; multipliez ce chiffre par trois pour avoir les investissements nécessaires. La deuxième chose est l'échelle. Le cloud public repose sur la mutualisation des ressources. Plus on opère à grande échelle, plus on peut tirer profit de ce facteur de mutualisation. La seule échelle viable pour un fournisseur de cloud public aujourd'hui, c'est l'Europe.

Quelques remarques. Non, le combat du cloud n'est pas perdu. C'est le lobbying des Américains qui le prétend. Non seulement il n'est pas perdu, mais il est plus important que jamais, car aujourd'hui, toute l'innovation européenne, ou presque, est dépendante du cloud. De plus, le cloud européen génère des retombées locales : un euro dépensé chez Scaleway, c'est 68 centimes qui restent en Europe ; un euro dépensé chez les *hyperscalers*, c'est moins de 20 centimes. Cela fait une grande différence.

Ce lobbying américain répète à qui veut l'entendre que l'offre n'est pas au niveau et que les clouds souverains sont plus chers. Ces deux affirmations sont fausses. J'en veux pour preuve que l'offre est disponible : chez Scaleway, nous couvrons 90 % des cas d'usage. Pour les 10 % restants, nous développons à la demande, comme nous le faisons pour France Télévisions, avec qui nous développons en partenariat les services vidéo qui manquent à notre boîte à outils. Deuxièmement, en moyenne, nous sommes presque 40 % moins chers que les *hyperscalers*. Quand on connaît leur niveau de marge, ce n'est pas le plus difficile.

En revanche, reconquérir la chaîne de valeur est effectivement complexe. Notre métier, c'est le logiciel. En dessous, il y a le hardware. Nous n'avons pas beaucoup de fournisseurs de serveurs en Europe, ce qui manque pour construire des clouds réellement souverains et indépendants technologiquement. En dessous des serveurs, il y a les data centers. Aujourd'hui, opérer dans des data centers européens à capital européen est de plus en plus difficile. Cela fait partie de notre promesse chez Scaleway, mais il y a de moins en moins de capitaux européens investis dans les data centers français. J'en veux pour preuve la part des capitaux européens dans les 109 milliards annoncés par le président Macron lors de Choose France pour la construction de centres de données. Mettre des clouds européens dans des data centers américains, c'est prendre le risque qu'ils soient coupés.

En un mot pour conclure, ce que nous attendons des pouvoirs publics, c'est une commande publique exemplaire et, surtout, une harmonisation réglementaire au niveau européen, car c'est la seule échelle viable pour un fournisseur de cloud public. Merci de m'avoir écouté.

M. le président Philippe Latombe. J'aurais peut-être une première question, avant de passer la parole à la rapporteure, qui fait écho à ce que vous avez dit, monsieur Lucas, et sur laquelle j'aimerais avoir votre vision à tous. Il y a quelque temps, le secrétaire d'État au numérique, Cédric O, nous disait que le combat du cloud était perdu et qu'il fallait passer à autre chose, comme le quantique et l'IA. D'autres auditions, comme celle de M. Lucas, nous

ont dit le contraire : le cloud n'est pas mort, il faut investir. La Commission européenne semble abonder dans ce sens avec son appel d'offres de 180 millions d'euros. Pourtant, nous avons encore entendu, pas plus tard que ce matin de la part de BPIFrance, et il y a quelques jours de la part de la directrice générale de France Digitale, que la bataille du cloud est finie.

Ma première question est donc la suivante : partagez-vous l'avis de M. Lucas selon lequel le cloud n'est pas mort ? Je suppose que votre présence ici le confirme. Mais au-delà du discours américain, pourquoi un certain nombre de personnes continuent-elles à défendre cette idée, et comment pouvons-nous, comme l'a suggéré M. Klaba, retrouver un récit ou une capacité à expliquer que ce n'est pas le cas ?

M. Octave Klaba. Pour éclaircir ce point, le cloud est une boîte à outils logicielle adossée à une capacité matérielle. Vous ne pouvez pas faire d'IA aujourd'hui si vous ne disposez pas de cette boîte à outils. Les entreprises américaines qui développent de l'IA utilisent le cloud pour le faire à grande échelle et sans réaliser d'investissements massifs, car leur métier reste le logiciel, et non la gestion de data centers ou les dépenses d'investissement, qui relèvent d'une autre typologie de métier.

On peut bien sûr essayer de faire de l'IA ou du quantique, mais l'ensemble de notre économie repose sur des données. Ces données, il faut les stocker, les transformer, les diffuser, et peut-être les utiliser pour l'IA ou à d'autres fins. Si vous n'avez pas toutes ces capacités de transport et de stockage de l'information, vous n'avez pas le reste. Vous ne pouvez pas faire d'intelligence artificielle. Il ne s'agit donc pas de l'un ou de l'autre ; ce ne sont pas deux choses différentes. L'IA est un service complémentaire sur le cloud, un outil de plus que nous ajoutons pour que nos clients, les développeurs, puissent créer des applications. Si demain vous leur proposez uniquement l'IA, ils vous diront qu'il manque tout le reste pour pouvoir développer leurs applications.

M. Philippe Miltin. Je pense qu'il y a plusieurs sujets. Le premier est que lorsque des personnes vous disent que le cloud est mort, elles ont été influencées par des acteurs américains qui affirment une chose vraie : « On ne peut pas nous remplacer ». En effet, aujourd'hui, si l'on considère la profondeur de leur catalogue de services et leurs dizaines, voire centaines de milliards d'investissements, l'ensemble des acteurs autour de cette table ne peuvent pas les remplacer du jour au lendemain. La réponse est non.

Cependant, ce n'est pas le sujet. Le sujet est de savoir si nous sommes en capacité de développer des outils logiciels, comme l'ont rappelé Damien Lucas et Octave Klaba, pour opérer un certain nombre de solutions, notamment critiques. La réponse est oui, et nous le prouvons absolument tous les jours, en France, en Europe et dans le monde. Chez Dassault Systèmes, de plus en plus de pays nous demandent de fournir une solution dite souveraine, en dehors des *hyperscalers*, parce que nous disposons de ces capacités, avant tout d'un point de vue logiciel. Nous opérons notre propre orchestrateur et hyperviseur, développé par Outscale, et cette capacité à fournir une boîte à outils est un élément extrêmement important. Nous savons le faire. Nous avons toutes les capacités en termes d'ingénierie système. Il faut avoir à l'esprit que les mathématiques françaises sont parmi les plus réputées, et nos ingénieurs sont très recherchés en France comme à l'étranger. Nous avons toute cette capacité de développement.

C'est toujours le sujet de la complémentarité. Si l'on parle de remplacer directement des *hyperscalers* qui génèrent plusieurs centaines de milliards en Europe, évidemment que non, nous ne pouvons pas le faire du jour au lendemain. Mais ce n'est absolument pas le sujet. Le sujet, aujourd'hui, est de savoir comment nous allons opérer des solutions critiques et des

données sensibles pour l'ensemble des opérateurs et des clients. De plus en plus de clients industriels viennent nous voir pour développer des solutions complémentaires. Une fois de plus, nous n'allons pas remplacer du jour au lendemain l'ensemble des *hyperscalers*. Nous avons toutes les capacités en termes de cloud public, de logiciels et d'infrastructures. Pour l'infrastructure, nous savons nous approvisionner en double source, que ce soit en Europe, aux États-Unis ou en Asie. Il est absolument invraisemblable d'entendre que le cloud est un sujet terminé. Au contraire, c'est un sujet d'actualité en France, en Europe et dans le monde.

M. Damien Lucas. Peut-être une hypothèse de réponse à la question du « pourquoi ». Mon hypothèse est que ce discours prend particulièrement bien parce que l'on craint les investissements. Le marché du cloud public en Europe représente au moins 80 milliards d'euros annuels. Il faudrait corriger au moins 50 milliards de ce montant pour que l'écosystème européen ait une part correcte. Cela représente donc 50 milliards de croissance pour les acteurs européens, soit 150 milliards d'investissements à trouver. Je pense que cette équation fait peur à beaucoup de monde, et il est beaucoup plus facile de se dire que l'on passe à autre chose.

Mais pour répondre à votre deuxième question, on ne pourra pas passer à autre chose tant qu'on n'aura pas réglé le problème du cloud. Octave Klaba l'a expliqué : il n'y a pas d'IA sans données, et les données sont dans le cloud, donc il n'y a pas d'IA sans cloud. La transitivité est simple mais brutale. Pour le quantique, je ferai appel à un autre élément. Si vous regardez la complexité des infrastructures, il y a dix ans, un serveur pouvait être installé dans le local de ménage d'une entreprise. Aujourd'hui, un GPU, compte tenu de sa consommation et des technologies de refroidissement, n'a pas d'autre solution que d'être placé dans un data center, voire dans un cloud. Après-demain, quelles entreprises pourront se payer et héberger un ordinateur quantique ? Pas beaucoup. Aujourd'hui, qui peut le faire ? Les fournisseurs de cloud. Ce sont les seuls. Et demain, ce sera pareil. Pas de cloud, pas de quantique. Si l'on veut fournir de la capacité de calcul quantique aux entreprises européennes, il faut des fournisseurs de cloud.

M. Éric Haddad. Je vais essayer de proposer un point de vue un peu nuancé, car l'idée que le cloud est fini peut être perçue comme vraie. En réalité, il se transforme. Le cloud, tel qu'il a été développé d'un point de vue technique et commercial à partir de la fin des années 2010, correspondait à ce qu'on appelait le « move to cloud ». Pour des raisons économiques, on transférait des cas d'usage ou des applications vers un cloud externe. Les Américains ont bien capté cette valeur, car ils ont été capables, avec les économies d'échelle qui ont été rappelées, d'offrir une offre permettant de capter ce transfert à un prix moyen plus bas, grâce à des contrats pluriannuels de plusieurs dizaines ou centaines de millions d'euros qui leur permettaient de fidéliser leurs clients. Je pense que ce marché est en train de se terminer ou, en tout cas, qu'il est en décroissance par rapport à ces premières années.

En revanche, un nouveau marché du cloud se développe en parallèle. C'est celui de la donnée et de l'IA. La bonne nouvelle pour nous, Européens, est que, qui dit donnée, dit souvent donnée sensible. Le curseur est subjectif ou objectif, mais d'une façon générale, on a toujours de bonnes raisons de considérer que la donnée est sensible, auquel cas il faut qu'elle soit gardée et traitée de façon locale ou, en tout cas, au niveau européen. C'est pourquoi je pense, et nous le voyons à notre échelle, que la plupart des cas d'usage, probablement les deux tiers, sont des demandes de clients et d'institutions liées à la donnée et à l'IA. Toutes ces données d'économie nous permettent d'augmenter la productivité et d'améliorer la relation avec les clients ou les citoyens.

Tout cela représente une opportunité pour nous, Européens. Il ne faut surtout pas se laisser endormir par l'idée que le cloud est fini. Oui, l'ancien cloud est peut-être fini, mais le nouveau est fantastique et formidable. Il faut capter cette valeur très rapidement.

Je voudrais ajouter un point à ce qui a été dit par Octave Klaba et Damien Lucas : la clé du succès réside probablement dans la mutualisation, la consolidation et la capacité à monter en échelle au niveau de l'infrastructure. Il faut absolument que nous maîtrisions la citoyenneté de nos data centers et que nous puissions gagner en échelle sur la notion d'infrastructure. Que nous soyons ensuite plusieurs à proposer des offres de valeur au-dessus de cette infrastructure mutualisée et consolidée, c'est un autre sujet. Mais objectivement, si l'infrastructure n'est pas à l'échelle européenne et si elle ne peut pas être mutualisée pour un nombre important d'offreurs, notamment de logiciels et de plateformes, la comparaison avec la capacité capitalistique des Américains ou des Chinois sera compliquée.

M. Sébastien Lescop. On pourrait poser la question différemment : ce combat du cloud peut-il être perdu ? Deux mouvements se réalisent en parallèle. Le premier, pour paraphraser mes confrères, est que le cloud fait aujourd'hui tourner l'économie du numérique, *deep tech* incluse. C'est important de le comprendre : sans le cloud, même si nous avons les meilleures innovations applicatives, nous ne saurons pas les faire tourner. Nous n'aurons pas cette liberté d'action. Le deuxième mouvement est un transfert de plus en plus fort de la valeur métier, en particulier de nos secteurs stratégiques qui portent aujourd'hui le PIB français, vers le numérique, valeur qui quitte le territoire français puisque les Français sont aujourd'hui de faibles producteurs de numérique.

Il est important de comprendre qu'il y aurait deux impacts à perdre cette guerre – qui pour l'instant n'est qu'une bataille, et nous sommes tous confiants autour de la table sur ce combat générationnel. Le premier est un impact économique fort, car cela va drainer énormément de valeur hors de l'économie française. Le deuxième est que, pour nos secteurs stratégiques, c'est aussi un enjeu de liberté, celle de pouvoir décider de leur avenir. Si une partie de leur capacité décisionnelle et de leur capacité de production est numérisée et qu'elle n'est plus détenue par des acteurs français, on peut se poser la question de la pérennité de leur capacité à décider et à innover.

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. Pour poursuivre la question du président et vos réflexions, vous l'avez dit, l'un des arguments utilisés pour affirmer que la bataille du cloud était perdue concerne l'offre de services. Il revient souvent que les offres européennes et françaises n'auraient pas les mêmes niveaux de service. Cela rejoint d'une certaine manière le bilan de la doctrine « cloud au centre » qui a été fait au mois de février par la direction interministérielle du numérique (Dinum), qui a conclu que les besoins concernent aujourd'hui la couche de services managés à développer. Que pensez-vous de cette analyse et que répondez-vous sur cette question du besoin d'étendre les services associés aux offres de cloud françaises et européennes ?

M. Damien Lucas. Je prends volontiers la parole sur ce sujet. Je pense qu'il y a un aspect historique. La France et l'Europe ont été pionnières en matière d'hébergement de serveurs. En 1999, OVH, Scaleway et quelques autres étaient en avance sur les Américains. Peut-être que l'Europe a un peu tardé à construire cette couche que nous appelons dans notre jargon le PaaS, les services managés (*Platform as a Service*). Si ce constat était vrai il y a cinq ans, il ne l'est plus aujourd'hui. Désormais, tous autant que nous sommes, nous avons

développé cette offre de services managés. Seuls ou en consortium, nous savons répondre aux besoins de la Commission européenne, comme cela a été annoncé vendredi. Nous savons répondre aux besoins de la Dinum, comme elle l'a annoncé. Nous savons répondre aux besoins des grandes entreprises françaises qui font le choix, peut-être courageux, de ne pas choisir les Américains.

Il y a vingt ans, on disait « *Nobody got fired for choosing IBM* ». Je pense qu'aujourd'hui, on pourrait appliquer cet adage en remplaçant IBM par AWS. La réalité est que les offres sont là et que cela a été démontré à plusieurs reprises. Le lobbying américain est très fort. Pour en donner une idée, les services managés d'AWS représentent probablement 600 services. Quelles sont les entreprises qui ont envie de faire une comparaison service par service sur 600 services pour vérifier si, chez Scaleway, OVH, Outscale, NumSpot ou CloudTemple, ces 600 services sont présents ? Il est beaucoup plus facile de rester là où l'on sait qu'ils sont.

Mme Cyrielle Chatelain, rapporteure. Vous avez évoqué deux sujets concernant les offres hybrides : la dépendance technologique, avec le risque du *kill switch*, et la question des data centers et des capitaux. Pourriez-vous développer un peu les risques contenus dans cette dépendance technologique et ce *kill switch* ? Dans certaines auditions que nous avons pu avoir, ces risques ont été relativisés. Votre analyse m'intéresserait. Sur l'autre sujet, vous avez souligné l'importance d'héberger vos services dans des data centers à capitaux européens. Quel est l'enjeu derrière cela ?

M. Philippe Miltin. Si je peux me permettre, sur la partie *kill switch*, je voudrais surtout aborder l'angle du *pricing power*. Au-delà du *kill switch* – même si un exemple est arrivé dernièrement avec la Cour pénale internationale (CPI) –, le sujet absolument majeur est l'augmentation permanente des prix imposée par les éditeurs américains, dont les entreprises européennes sont de plus en plus dépendantes. Au-delà des sujets d'IA qui vont devenir essentiels, se dégager de cette dépendance vis-à-vis des éditeurs américains est crucial. Il y a eu l'affaire VMWare-Broadcom, mais au-delà de cela, il y a des augmentations significatives et permanentes chaque année, qui créent une dépendance extrêmement forte.

On a parlé des 600 services d'AWS, mais lorsqu'une entreprise a développé l'ensemble de ses solutions autour de ces services, en sortir est extrêmement compliqué. La réversibilité et l'interopérabilité ne sont absolument pas des sujets maîtrisés par nos amis américains. Ces enjeux sont aujourd'hui majeurs, non seulement pour permettre à l'économie européenne de perdurer, ce qui est vital, mais aussi pour contrer ce pouvoir sur les prix qui est, pour moi, l'élément le plus déterminant.

M. Éric Haddad. Je reviens sur votre première question. Je pense que les 600 ou 200 services, selon l'offreur américain, sont plus un argument de vente contractuel, un moyen de créer une adhérence entre le fournisseur et l'acheteur. On parle beaucoup d'adhérence technologique, mais je pense qu'il y a une très forte adhérence économique liée à l'achat et aux contrats pluriannuels. L'un des moyens de justifier un bon projet d'achat est cette quantité de services qui, en réalité, seront très peu utilisés. Damien Lucas a tout à fait raison : la panoplie de services que nous proposons est très largement suffisante, et quand elle ne l'est pas, nous nous arrangeons avec le client pour développer ce qui est nécessaire.

Le vrai sujet n'est pas là. Le vrai sujet est la capacité de négociation à grande échelle des Américains, la construction de grands contrats pluriannuels, où le nombre de services et la diminution apparente du coût sur le volume servent d'arguments de vente, mais renforcent

l'adhérence. Il est extrêmement difficile, au-delà de l'adhérence technologique, de sortir d'un contrat sur lequel on s'est engagé pour quatre ou cinq ans. C'est une réalité, surtout quand le commercial revient vous voir un ou deux ans avant la fin pour renégocier, en arguant qu'il serait dommage de ne pas profiter de la baisse des prix sur le volume. En tant que bon acheteur, vous signez un bon contrat. C'est une logique d'adhérence qui se poursuit indéfiniment.

C'est pourquoi, objectivement, il est extrêmement compliqué pour des acteurs comme nous d'avoir un argumentaire convaincant dans le secteur privé, au-delà du fait que le *move to cloud* est en train de s'étioler. C'est là où l'État a un rôle d'exemplarité à jouer pour montrer qu'il est possible de sortir de cette logique d'achat, de profiter des nouveaux usages liés à la donnée, où il y a un vrai besoin de gestion des données sensibles et de souveraineté, et de créer une rupture avec ces adhérences économiques et ces logiques de services d'achat.

M. le président Philippe Latombe. Pour prolonger la question de la rapporteure, prenons l'exemple de ce qui s'est passé avec la Commission européenne et son appel d'offres de 180 millions d'euros. Ce qui est assez impressionnant, c'est que sur les quatre attributaires, beaucoup ont répondu en consortium. Il y a très peu d'entreprises qui ont répondu de façon individuelle. OVH, par exemple, a répondu avec Clever Cloud et un autre partenaire. On l'a vu aussi un peu sur le Health Data Hub, où quelques consortiums s'étaient formés.

J'ai deux questions en une. Premièrement, avez-vous intégré cette logique de consortium pour améliorer votre offre de services en profitant des complémentarités de chacun ? Travaillez-vous ensemble de temps en temps, sans vous voir uniquement comme des concurrents ? Deuxièmement, avez-vous le sentiment que les acheteurs, tant publics que privés, sont de plus en plus dans cette logique d'accepter des consortiums, au lieu de vouloir un seul contrat avec une seule personne qui fournit l'intégralité des services ? Sentez-vous ce changement de paradigme, aussi bien dans le secteur privé que dans le secteur public ?

M. Octave Klaba. Pour répondre à la question sur la Commission européenne, nous avons répondu en consortium pour une raison simple : nous avions une relation établie avec Deep depuis deux ou trois ans. Deep était venu témoigner à notre sommet sur des développements que nous avions faits avec eux, car ils ont une certaine ambition pour le cloud au Luxembourg. Il se trouve qu'ils avaient formé un consortium avec Clever Cloud pour répondre à la Commission européenne. Comme nous nous entendions très bien avec Deep et Clever Cloud, j'ai décidé d'explorer cette possibilité de travailler dans un cadre très innovant pour nous. C'est très disruptif pour une entreprise comme OVHcloud de construire une réponse à trois. C'était intéressant de devoir se mettre d'accord. Maintenant, le vrai travail va commencer, car ce n'est que l'ouverture du contrat ; il faut maintenant aborder la partie légale, la facturation, puis aller voir toutes les agences et travailler sur chaque contrat. Cela m'a intéressé d'explorer où cela pouvait nous mener. C'était une certaine prise de risque pour nous, car nous aurions très bien pu répondre seuls ; d'ailleurs, nous nous étions fait référencer comme candidat possible et avons retiré notre candidature pour rejoindre le consortium.

Pour répondre à votre deuxième question, c'est très intéressant car on observe des comportements un peu différents. Souvent, les fournisseurs de cloud répondent avec un partenaire, mais nous ne sommes pas le contractant principal. C'est le partenaire qui répond à l'appel d'offres et qui embarque un fournisseur de cloud. Cependant, il nous arrive de plus en plus souvent qu'on nous demande d'être le contractant principal et de prendre la responsabilité non seulement du cloud, mais aussi du développement pour répondre aux besoins du client. Nous sommes en train d'expérimenter ce type de réponse pour voir ce que cela implique

juridiquement et en termes de livraison, et si les expériences sont bonnes. Je n'ai pas d'avis tranché aujourd'hui.

Souvent, les fournisseurs de cloud sont en arrière-boutique, en support d'un partenaire. Très rarement, nous nous mettons en avant car nous ne prenons pas la responsabilité finale du produit livré ; c'est notre partenaire qui utilise le cloud pour assembler la solution dont le client final a besoin. Surtout, le partenaire connaît très bien le client lui-même, il a investi beaucoup de temps dans la relation finale. Nous ne sommes pas censés avoir cette intimité avec les clients dans la chaîne de valeur. Mais c'est en train de changer. J'ai parlé de 1,2 milliard d'euros de chiffre d'affaires et de notre ambition d'aller à deux milliards. Nous nous posons ces questions : quel est notre rôle dans la chaîne de valeur ? Jusqu'où devons-nous le remettre en question ? Quel est le rôle des partenaires ? Faut-il réinventer ce rôle et cesser d'être un acteur passif pour devenir plus actif, car certains clients le demandent ?

M. Damien Lucas. Pour revenir sur la question des offres hybrides, je voudrais souligner un point, car soit il y a quelque chose que je n'ai pas compris, soit je vais être extrêmement jaloux. J'ai entendu dire que certaines offres hybrides imaginaient, en cas de coupure des mises à jour, pouvoir faire fonctionner leur cloud pendant un an sans recevoir de correctifs de leurs partenaires américains. Alors là, je ne sais pas comment ils font. Chez Scaleway, nous faisons 72 mises à jour quotidiennes, dont une proportion non négligeable sont des mises à jour de sécurité. Je vois donc deux options : soit ils ont une technologie incroyable que je ne connais pas, soit ils connaissent déjà toutes les failles de sécurité qui seront découvertes dans les douze prochains mois et les ont déjà corrigées. Mais il y a quelque chose que je n'ai pas compris, et je pense qu'on n'a pas poussé l'exercice jusqu'au bout sur ce sujet.

M. le président Philippe Latombe. Peut-être est-ce parce qu'ils ont tout mis en avance de phase et qu'ils ont tout expérimenté.

M. Damien Lucas. Je savais que je ferais bien de venir aujourd'hui.

Sur votre question concernant les data centers, nous, fournisseurs de cloud, opérons tous dans des data centers. Or, il est extrêmement simple de les éteindre ; c'est un véritable *switch*. Avoir des data centers dont le capital de l'entreprise qui les détient n'est pas européen, c'est soumettre tous les flux de travail à cette menace de coupure. Je suis évidemment d'accord avec Philippe Miltin : cette question du *kill switch* ne sera peut-être jamais utilisée, mais pensez au soft power que représente la seule menace de pouvoir couper. Et gardez à l'esprit que la plupart des data centers en Europe sont de nationalité étrangère. S'ils décident de les éteindre, nous n'avons pas grand-chose pour nous y opposer.

Sur votre dernière question concernant les consortiums, je serai peut-être le mouton noir de l'assemblée. Chez Scaleway, nous n'y croyons pas. C'est trop compliqué. Nos clients cherchent une alternative à AWS, à GCP (Google Cloud Platform) ou à Azure. Ils ne cherchent pas un conglomérat de multiples petites entreprises – un acteur pour la France, un autre pour la Belgique, un autre pour l'Allemagne, etc. Ils ne cherchent pas un consortium avec un acteur pour l'infrastructure et un autre pour les services managés. Ils cherchent juste une alternative crédible et à l'échelle à leur fournisseur actuel. Car reconnaissons-le, en dehors du prix et des pratiques commerciales où le droit européen est régulièrement bafoué, nos clients adorent le service proposé par AWS, GCP et Azure. Ils veulent juste des alternatives européennes qui respectent le droit commercial en Europe.

M. le président Philippe Latombe. C'est bien d'avoir un avis différent, cela me va bien.

M. Éric Haddad. Je pense que la notion de consortium est contextuelle. L'appel d'offres européen était un cas particulier. Pour chaque contexte de client ou d'appel d'offres, on peut effectivement travailler en consortium. En tout cas, chez NumSpot, nous le faisons nativement, au-delà même de notre structure capitalistique. Je pense qu'il est bénéfique pour les clients de se constituer en consortium, en partenariat, en écosystème, pour être capable d'apporter une réponse intelligente. Je pense que cela va s'arrêter là. Quant à savoir si cela peut se poursuivre de façon plus structurelle, je n'en sais rien, mais de façon contextuelle, pour répondre à un marché et pour être plus fort face à des entreprises très organisées et capitalistiquement plus puissantes, ce n'est pas stupide.

M. Philippe Miltin. Je voulais juste ajouter que si la Commission européenne ou des acteurs privés sont prêts à étudier le sujet du consortium, c'est que ce sujet devient tellement critique pour eux que toutes les solutions sont envisageables. Effectivement, avoir un seul fournisseur est ce qu'il y a de mieux. Mais de temps en temps, pouvoir s'appuyer sur plusieurs acteurs pour couvrir plusieurs pays avec plusieurs offres de services, ce sont des choses qui sont envisagées aujourd'hui. Et si elles le sont, c'est que le sujet est devenu si important que les choses se font.

M. Sébastien Lescop. Je voudrais juste rajouter un complément sur les data centers. Il faut savoir que les data centers sont ceux qui revendent l'électricité. Aujourd'hui, nous avons la chance en France d'avoir une offre d'électricité compétitive et décarbonée. Il y a donc une question sur la préemption et la captation à la source de cette valeur française par des data centers étrangers, dans lesquels demain il y aura peut-être des fournisseurs de cloud. Il faut s'assurer que cette valeur sera bien redistribuée à l'écosystème technologique, mais également aux consommateurs. C'était une ouverture. Je pense qu'aujourd'hui, nous avons suffisamment de capacité en data centers, je parle pour les trois prochaines années, pour avoir une émulation et une compétition qui nous protègent d'une augmentation significative de nos prix d'électricité. Mais qu'en sera-t-il demain, lorsque nous commencerons peut-être à avoir une saturation du marché ?

Mme Cyrielle Chatelain, rapporteure. Mes questions porteront sur deux thèmes distincts. Le premier concerne les investissements. Vous avez évoqué à plusieurs reprises dans vos propos la question de l'investissement et de la masse d'investissements à réaliser. Selon vous, par qui ces investissements doivent-ils être portés ? Est-il nécessaire de prévoir un apport de fonds publics ? Ou, à l'inverse, la solution réside-t-elle dans la structuration de capacités d'investissement de capitaux privés européens ? Quelle est également votre propre part dans ces investissements ? En somme, pour atteindre le niveau d'investissement requis, qui doit, selon vous, amorcer cette augmentation significative, même si des investissements sont déjà en cours ?

Ma deuxième série de questions porte sur les référentiels. Nous disposons avec SecNumCloud d'un référentiel assez unique en Europe. Le jugez-vous satisfaisant ? Est-il aujourd'hui stabilisé et permet-il de stocker, notamment, les données les plus sensibles des administrations ? Par ailleurs, comment envisagez-vous son évolution ? Une réglementation européenne sur les questions du cloud est attendue. Or, jusqu'à présent, dans le cadre du schéma européen de certification des services de cloud, nous n'avons pas réussi à intégrer un aspect de souveraineté dans la certification. Nous avons manqué la première étape ; il faut espérer ne pas manquer la seconde. Avez-vous des échanges à ce sujet au niveau européen ? Quelles sont les

perspectives ? L'appel à projets témoigne-t-il déjà de la prise en compte de cette nécessité de mettre en avant les enjeux de souveraineté ?

Enfin, existe-t-il d'autres référentiels intégrant la notion de souveraineté ? Par exemple, la certification Hébergeur de données de santé (HDS), qui comporte un certain nombre d'exigences mais pas celle d'être développé par des compagnies françaises ou européennes, pourrait-elle permettre d'orienter une partie de la commande, notamment privée, vers des offres de cloud françaises ou européennes ?

M. le président Philippe Latombe. Pour un simple complément de question, la fusion ou le rapprochement du référentiel HDS et de la qualification SecNumCloud serait-elle une bonne solution ?

M. Octave Klaba. Concernant les investissements, j'ai la conviction que ce n'est pas au domaine public de porter les investissements d'entreprises privées. Celles-ci doivent assumer une part du risque, c'est leur métier. De plus, il faut savoir que les capitaux disponibles sont abondants et ne demandent qu'à être investis, pourvu que les projets présentent des perspectives de revenus. La véritable problématique réside dans la capacité à générer des revenus et à obtenir des engagements suffisants pour soutenir les investissements, que ce soit en fonds propres, en dette ou par d'autres moyens. On évoque les milliards investis par les acteurs américains, mais il faut analyser correctement leurs comptes de résultat, car on mélange deux choses. Il existe deux types d'investissements. Le premier relève du fonctionnement courant, le « business as usual ». Ces investissements sont obligatoires pour conserver des clients sur des produits existants ; il s'agit de renouveler des équipements, comme des serveurs qui ont une certaine obsolescence, ou d'ajouter de nouvelles ressources pour accompagner la croissance. Plus de 90 % des investissements annoncés relèvent de cette croissance ou du fonctionnement courant. Les chiffres qui peuvent donner le tournis ne représentent que leur activité normale. Il ne s'agit pas, dans leur bilan, d'une prise de risque démesurée dans des technologies qui n'existent pas encore. C'est simplement l'investissement nécessaire pour acquérir de nouveaux clients et assurer la croissance de leur revenu sur des produits existants.

En distinguant bien cette partie, je peux prendre notre exemple : sur un investissement de 350 millions d'euros, environ 70 millions sont investis dans le logiciel. Nos informations sont publiques, l'entreprise étant cotée. Cela correspond aux salaires des développeurs. Sur un peu plus de 3 000 personnes dans l'entreprise, nous avons 1 000 développeurs, 1 000 personnes à la production dans les centres de données et 1 000 personnes dans les fonctions commerciales. Je capitalise donc environ 70 millions d'euros par an, qui sont dédiés au développement de nouveaux produits. Le reste, soit la différence par rapport aux 350 millions, concerne les centres de données et le matériel que je renouvelle ou que j'ajoute pour la croissance.

La qualification SecNumCloud est complexe à mettre en œuvre. Je la trouve cependant très intéressante, car elle est axée sur la cybersécurité d'un point de vue technique, ce que les autres réglementations ne font pas. Celles-ci imposent généralement des processus aux entreprises, avec des audits pour vérifier leur suivi. Dans le cas de SecNumCloud, il ne se limite pas à cela. Une part très importante concerne la manière de construire l'infrastructure, de chiffrer les données ou de gérer les accès clients. Le référentiel est contraignant, en ce sens qu'il n'accorde pas une liberté totale sur la manière de concevoir le produit ; il impose de le construire d'une certaine façon. C'est ce qui explique la longueur des délais d'obtention de la qualification SecNumCloud. Le problème n'est pas l'audit, mais le temps nécessaire pour adapter une technologie qui fonctionne de manière autonome en cloud public à l'ensemble des exigences de SecNumCloud. C'est en cela qu'il est très intéressant, et personne d'autre ne le fait en

Europe. Aucune autre autorité, que ce soit en Allemagne, en Italie ou ailleurs, n'impose une telle manière de procéder. Cette approche vient de l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui a capitalisé sur de nombreux retours d'expérience pour élaborer un manuel de bonnes pratiques visant à éviter des incidents comme ceux survenus dans les hôpitaux, avec des rançongiciels et autres attaques. C'est un guide de bon sens pour construire et opérer un cloud destiné à l'État, aux données extrêmement sensibles, aux besoins militaires ou à d'autres usages critiques. C'est en cela que je trouve une valeur incroyable à ce qui a été construit par l'Anssi. Nous l'utilisons de cette manière et nous essayons bien sûr d'obtenir les certifications pour monétiser commercialement tout le travail accompli. Mais ce travail de cybersécurité est extrêmement intéressant à analyser, à approfondir pour élaborer des offres dans cet état d'esprit.

Enfin, concernant la fusion de la certification HDS et de la qualification SecNumCloud, j'en serais personnellement très satisfait, car nous détenons SecNumCloud. Je pense cependant que beaucoup d'acteurs protesteraient, car la certification HDS n'est pas très complexe à obtenir. Elle repose sur la norme ISO 27001, à laquelle on ajoute deux ou trois processus. SecNumCloud est d'une tout autre nature ; il s'agit véritablement d'une approche militaire du cloud. Imaginez que votre cloud soit sur un champ d'opérations et que vous perdiez les conteneurs dans lesquels il se trouve. Si l'ennemi saisit ces conteneurs alors que le système est toujours en fonctionnement, peut-il récupérer les données ? Peut-il utiliser ce qui tournait dessus ? Quelles mesures mettez-vous en place pour que personne ne puisse récupérer les informations, y compris avec un tournevis ou n'importe quel autre moyen ? C'est cela, le niveau d'exigence de SecNumCloud. Et c'est unique.

M. le président Philippe Latombe. L'actualité nous montre que des questions de cybersécurité émergent quotidiennement. C'est également une demande forte pour les données les plus sensibles.

M. Damien Lucas. Pour commencer sur la question des investissements, comme l'a très justement dit Octave Klaba à l'instant, il y a deux types d'investissements pour un fournisseur de cloud : l'investissement dans les ressources humaines pour développer les technologies d'avenir, et l'investissement dans les infrastructures pour héberger les workflows de nos clients.

Sur la partie humaine, les différentes initiatives, y compris l'appel à projets sur le renforcement de l'offre de services cloud, sont bienvenues, car elles aident à continuer d'investir et à développer de nouveaux produits innovants. Mais la très grande majorité des investissements concerne les infrastructures. Et je ne crois pas que ces investissements d'infrastructure doivent être financés par de l'argent public. Ils doivent être adossés à des engagements de commandes, à un marché florissant, pour pouvoir être financés par de la dette ou par des fonds à moindre risque, car le carnet de commandes suit. C'est en s'engageant sur des volumes de commandes, comme l'a fait la Commission européenne, que l'on crée la capacité à financer ces investissements avec de l'argent privé, que ce soit par la dette ou l'investissement, dans des conditions favorables. Je pense que ce montage est beaucoup plus intéressant pour aider à développer l'offre que de recourir à l'argent public. Nous parlons de dizaines de milliards d'euros d'investissements ; je ne crois pas qu'il soit sain aujourd'hui pour les différents États membres de l'Union européenne d'engager de telles dépenses, alors qu'elles pourraient être assumées par le secteur privé, à condition que le carnet de commandes soit au rendez-vous.

Pour revenir sur la question des différentes certifications et des référentiels, la première demande, comme je l'avais indiqué dans mon propos liminaire, est l'harmonisation au niveau européen. Rappelons-le, il n'existe pas d'échelle viable en dehors du marché européen. Si la France a SecNumCloud, l'Allemagne le C5 avec le BSI, et l'Italie l'ACN Level 1, cela signifie que pour un fournisseur de cloud, il faut passer les certifications vingt-sept fois dans le pire des cas. Aucun d'entre nous autour de cette table ne peut se le permettre. Seuls les géants du secteur, dont vous voyez à qui je fais allusion, en ont les moyens. Aujourd'hui, la fragmentation des différents référentiels retarde le déploiement du cloud européen et favorise les géants étrangers. Le premier point est donc l'harmonisation.

Le second point est qu'il ne faut pas, à mon sens, avoir un label unique binaire, de type « oui/non ». Un tel label signifierait soit que l'on place la barre très haut, comme avec SecNumCloud, qui est un bon référentiel, mais dans ce cas, le nombre d'offreurs en Europe serait extrêmement limité ; soit que, pour assurer une offre suffisante face à la demande, on abaisse le niveau d'exigence et l'on se met à autoriser des offres hybrides, voire des « AWS Sovereign Cloud » en Allemagne, dont on peut se demander d'où ils tirent le qualificatif de « souverain ». Mais là, on crée un problème. Je suis un fervent défenseur de l'approche de la Commission avec le Cloud Sovereignty Framework, qui permet de procéder à une évaluation selon différents axes, de manière que les entités ou les entreprises puissent ensuite faire leur choix en toute connaissance de cause, en fonction de la criticité de leurs données, plutôt que d'être face à un choix binaire « SecNumCloud ou rien ». Autrement, nous n'aurons pas assez d'offres pour répondre à la demande.

M. Philippe Miltin. Je suis entièrement en phase avec ce que viennent d'exposer MM. Klaba et Lucas : l'investissement doit être absolument privé. Si je prends le cas d'Outscale, nous avons la chance d'être financés par un leader mondial du logiciel, Dassault Systèmes, ce qui représente des centaines de millions d'euros d'investissement pour favoriser le développement du SaaS. Ce qui est intéressant dans cette situation, c'est que Dassault Systèmes met en œuvre l'intelligence artificielle pour tous ses clients en mode SaaS, partout dans le monde. Ces technologies, nous allons ensuite les distribuer en France et en Europe. Il est évident que la demande de la part des clients privés pour des technologies d'IA et de cloud souverain est de plus en plus forte, car la souveraineté est une attente locale, et ce au niveau mondial, pas seulement en France ou en Europe. Ces développements sont financés parce qu'il y a un modèle économique derrière, celui du SaaS. Cela est normal et doit se faire ainsi.

Les appels à projets sont évidemment importants pour nous aider à accélérer notre développement, mais il faut aussi pouvoir les flécher sur quelques champions. Le morcellement actuel est mortel, car si nous avons besoin d'aide, il faut le faire de façon significative et non dispersée. Je pense que c'est extrêmement important.

Le dernier point que je voulais ajouter est que je suis aussi tout à fait d'accord sur la nécessité d'avoir une certification européenne. Nous n'avons pas les moyens d'obtenir toutes les certifications nationales. Mais il faudrait aussi ajouter quelques critères aux référentiels. Par exemple, le critère intégrant les exigences d'indépendance technologique nous semble important pour la résilience et pour maîtriser notre *pricing power*, afin de ne pas être dépendants. Le fait de repeindre en bleu, blanc, rouge ou aux couleurs de l'Europe des technologies américaines ne confère aucune indépendance technologique. Je pense que ce sont des critères qui doivent être ajoutés, au-delà de l'aspect cybersécurité, qui est, comme Octave Klaba l'a bien rappelé, un élément extrêmement important.

M. Éric Haddad. S’agissant de SecNumCloud, cette qualification a la vertu de clarifier le marché, de guider l’acheteur et de permettre d’objectiver une situation, notamment face au *sovereign washing* ou marketing agressif de certains acteurs qui se prétendent « justes et souverains ». C’est une façon d’objectiver les choses et de les rendre très claires pour les acheteurs.

Faut-il jumeler la certification HDS avec d’autres types de certifications comme SecNumCloud ? Je ne le crois pas. Il me semble plutôt intelligent de conserver un nivellement, car il y a un marché pour tous les profils et différents types d’acteurs. Effectivement, comme l’a dit Octave Klaba, développer une offre SecNumCloud est extrêmement coûteux du point de vue humain et financier en ingénierie, et tout le monde n’est pas prêt à le faire.

Faut-il une qualification ou une certification européenne ? Je le souhaiterais. Cependant, objectivement, bien que je ne suive pas ce dossier de près, cela me semble très ambitieux vu la fragmentation des positions en Europe. Si au moins nous avions un référentiel commun, ce serait une avancée. Par exemple, être qualifié SecNumCloud ou un équivalent dans son pays, complété par un ou deux autres critères, pourrait suffire pour permettre une expansion européenne qui ne soit pas trop onéreuse. Je pense qu’il faut être réaliste. Nous avons en France une bonne qualification, SecNumCloud, qui tient la route. Elle ne répond pas à tout, et contrairement à ce qui est écrit dans les journaux, il y a beaucoup d’amalgames. Il est important de clarifier à quoi elle sert et à quoi elle répond. Une qualification européenne serait idéale, mais si nous pouvions au moins avoir un référentiel commun, ce serait moins ambitieux mais nous permettrait d’avancer. Je pense que c’est ce qui a été fait récemment, même si l’acronyme m’échappe. C’est une bonne façon d’établir des critères pour une offre et de faire en sorte que les acteurs qui ont investi sur la souveraineté et l’autonomie numérique puissent être qualifiés de façon objective.

M. Sébastien Lescop. Concernant les financements publics, je voudrais revenir sur la dépendance technologique vis-à-vis des hyperscalers. On observe aujourd’hui une situation à deux vitesses. Pour les nouveaux projets, la loi Sren est très utile pour éviter les coûts de réversibilité et les crédits cloud. Néanmoins, il y a tout l’existant, qui constitue la plus grosse partie du marché. Lorsqu’un client a ses équipes formées sur une technologie propriétaire et que ses applications sont développées avec des API propriétaires, il devient extrêmement coûteux de quitter un *hyperscaler*. L’un des seuls moyens qui pourrait être utilisé pour réduire cette dépendance – je ne dis pas qu’il faut l’utiliser, mais c’est une option – serait de la financer, en augmentant artificiellement la compétitivité des acteurs français et européens.

Concernant la certification HDS, le monde de la santé est assez fragmenté. Il est vrai qu’imposer une rigueur telle que celle de SecNumCloud pourrait être destructeur pour l’innovation. Néanmoins, qui dit données de santé ne dit pas forcément données non sensibles. Certaines données de santé, comme des bases de données concernant des millions de Français, pourraient être considérées comme sensibles, car elles peuvent être la cible de cyberattaques et potentiellement déstabiliser un gouvernement. Il ne faut donc pas écarter la possibilité que les deux référentiels puissent s’appliquer à une même application et aux mêmes données.

Pour ce qui est de SecNumCloud, en tant que *pure player* de ce référentiel, nous en sommes naturellement partisans. Nous constatons que cette qualification est en train de devenir un standard de marché, en tout cas en France. Il y a un véritable engouement autour d’elle, et le directeur général de l’Anssi, M. Vincent Strubel, en parle très bien. Ce que nous pouvons constater, en tant que fournisseur, c’est que lorsque les exigences sont intégrées dès la conception, les surcoûts de production ne sont pas si importants.

Mme Cyrielle Chatelain, rapporteure. Je voudrais reformuler ma dernière question sur la certification HDS. J'ai bien compris que fusionner les deux labellisations serait probablement contre-productif et très compliqué pour certains acteurs. Cependant, des acteurs français qui cherchent à faire valoir leurs spécificités par rapport à des concurrents extra-européens plus petits qui parviennent à obtenir la certification HDS, nous disent qu'il est dommage de ne pas avoir un volet de souveraineté pour les données de santé. Sans aller jusqu'au niveau de cybersécurité de SecNumCloud, y aurait-il un intérêt, pour ces données de grande qualité et à la sensibilité spécifique, à favoriser les acteurs européens ou français en intégrant à la certification HDS une dimension de souveraineté ? Ou estimez-vous que cela reste complexe au vu du marché actuel ?

Ma deuxième question est d'un tout autre ordre et concerne le développement des centres de données et leur impact environnemental. Vous avez mentionné la consommation énergétique. Il est vrai que la consommation d'énergie et d'eau fait partie des préoccupations aujourd'hui grandissantes. Il y a un enjeu à disposer d'infrastructures en France, tout en parvenant à réduire leur impact environnemental. En effet, si l'on triple la capacité des centres de données en Europe, conformément à l'objectif de la Commission, la consommation énergétique dépasserait la production actuelle des capacités nucléaires installées en France. Nous parlons de quantités importantes. Pourriez-vous nous indiquer où vous en êtes de votre réflexion sur l'impact environnemental de ces infrastructures énergivores, ainsi que sur la question sensible de l'eau ?

M. le président Philippe Latombe. J'ai vu de nombreuses mains se lever et je vais donc exercer mon rôle de président en distribuant la parole. Je la donne d'abord à M. Klaba, puis à M. Lucas. L'ordre changera ensuite, ne vous inquiétez pas, je poserai une question qui vous permettra de commencer.

M. Octave Klaba. Je vais tenter de répondre à la deuxième question sur les centres de données. Nous avons fait le choix assez tôt, dès 2004, de posséder le terrain, le bâtiment et de concevoir tout ce qu'il y a à l'intérieur de nos centres de données pour une raison simple : nous voulions qu'ils soient plus écologiques et moins consommateurs d'énergie. Aujourd'hui, l'ensemble de nos centres de données fonctionnent avec nos propres systèmes de refroidissement par eau (*watercooling*). Nos 500 000 serveurs physiques partout dans le monde sont refroidis avec cette technologie. Cela nous apporte une réduction d'environ 50 % de la facture énergétique. Les chiffres sont publics : aujourd'hui, la facture énergétique d'OVH représente environ 5 % de notre chiffre d'affaires. Si nous n'avions pas le *watercooling*, cela représenterait 10 %.

Cette approche, que nous suivons depuis vingt ans, nous permet de réaliser des économies que nous répercutons sur nos clients, puisque nous sommes moins chers que nos concurrents. Ces 5 % de différence sur les prix constituent un très bon argument commercial. Pendant très longtemps, nos concurrents ont expliqué nos prix bas par une prétendue moindre qualité. Structurellement, nous avons mis en place des solutions qui permettent de réduire cette facture. Nous avons tout un système autour du refroidissement et de la circulation de l'eau. L'avantage est que nous avons des ingénieurs qui travaillent sur ce sujet en interne ; ce ne sont pas des technologies que nous achetons à l'extérieur. Nous avons des spécialistes en mécanique des fluides, en tuyauterie, et des experts dans tous les métiers que nous intégrons, puisque nous construisons nos propres centres de données. Nous sous-traitons l'exécution de la construction à des acteurs locaux pour maximiser l'impact local. Si nous déployons un centre de données en Pologne, en France ou en Italie, nous travaillons avec de petits sous-traitants locaux pour que

l'argent irrigue l'économie de la région. Nous aimons avoir cet impact social et régional. Mais toute la technologie vient de chez nous et nous en maîtrisons l'ensemble.

Nous avons une approche similaire concernant l'obsolescence des serveurs. Ceux-ci fonctionnent au maximum neuf ans. Au bout de cette période, il faut les sortir et en faire quelque chose. Nous avons tout un département qui récupère l'ensemble des pièces détachées et les recycle à travers différentes filières. C'est un système que nous avons mis en place depuis au moins douze ou treize ans et qui s'intègre dans le cycle de vie de nos investissements. D'un côté, nous investissons dans nos usines pour construire nos serveurs et nos baies, nous les envoyons dans les centres de données, puis nous les démantelons et les faisons repasser par les mêmes usines pour recycler l'ensemble des pièces. Tout cela est intégré au sein de l'entreprise.

C'est un ensemble de métiers que nous maîtrisons pour pouvoir opérer à grande échelle. Nous construisons 70 000 à 75 000 serveurs physiques par an dans nos deux usines en Europe et au Canada, ce qui nous donne la masse critique pour le faire. C'est rare. L'autre usine que je connais en France est celle de Bull ; sinon, il n'en existe pas. Nous sommes l'un des plus gros acheteurs de mémoire vive, de disques durs et de pièces détachées, et l'un des plus gros constructeurs de serveurs en Europe. Tout ce savoir-faire que nous avons ajouté à notre portefeuille de compétences nous sert aujourd'hui précisément sur ces enjeux. Nous faisons des économies, nous sommes plus écologiques, et grâce à cela, nous pouvons nous déployer. Par exemple, à Singapour, la construction de nouveaux centres de données est interdite depuis trois ou quatre ans. OVH a obtenu l'autorisation d'en construire parce que nos centres de données sont refroidis par eau. Nous avons bénéficié de dérogations car nous avons démontré que notre impact était moindre. C'est un avantage que nous ne mettons pas toujours en avant. Pendant très longtemps, nous n'en parlions pas, car on se faisait insulter : « Tu mets de l'eau dans les baies informatiques, mais tu es complètement dingue ! ». Il se trouve qu'aujourd'hui, vous avez l'obligation de le faire pour récupérer la chaleur. C'est devenu obligatoire dans les dernières générations de GPU, une chose que nous faisons à une autre échelle et avec un autre recul depuis une vingtaine d'années.

M. Damien Lucas. Je ne vais pas répondre à votre première question, mais je vais vous dire pourquoi. Sur la question d'intégrer un critère de souveraineté au référentiel HDS, je ne crois pas que ce soit une question pour les fournisseurs de cloud. C'est une question pour les citoyens. Les citoyens français acceptent-ils que leurs données de santé soient hébergées sur des clouds qui ne sont pas européens ? J'ai un avis en tant que citoyen, pas en tant que directeur général de Scaleway. En tant que directeur général, nous offrons la certification HDS, mais je ne crois pas que la question se situe à ce niveau. La vraie question est celle de la prise de conscience par le peuple français, et plus généralement européen, du risque pesant sur leurs données de santé.

Sur la question des centres de données, plusieurs éléments. Premièrement, chez Scaleway, à l'opposé de ce qu'a fait Octave Klaba, nous avons décidé d'arrêter de construire nos propres centres de données. Nous en avons fait beaucoup par le passé, en travaillant à les rendre très efficaces énergétiquement. Nous considérons aujourd'hui que nous préférons choisir les partenaires les plus efficaces en termes d'énergie pour notre expansion. De ce fait, deux constats s'imposent. Le premier est qu'en France, nous sommes à court de centres de données. Il n'y a plus de capacité disponible, et nous sommes obligés de nous déployer à l'étranger. Il n'y a plus de capacité dans des centres de données sur le sol français, et en particulier, il n'y a plus rien du tout dans des centres de données européens sur le sol français. Quand de la capacité sera à nouveau disponible, ce sera probablement chez des opérateurs étrangers installés en

France. De plus, à court terme, pour 2026-2027, il n'y a plus de capacité du tout. C'est un problème, car nous sommes contraints de nous tourner vers l'étranger.

Or, à l'étranger, la situation est généralement beaucoup moins favorable qu'en France, où nous bénéficions d'une électricité hautement décarbonée. Quand certains acteurs américains construisent des projets à l'échelle du gigawatt en brûlant du gaz de schiste dans des turbines, ce n'est pas très décarboné. Heureusement, en France, c'est interdit. Nous avons une électricité de bonne qualité. On parlait de la consommation d'eau : en France, il est interdit pour les centres de données de refroidir avec des tours qui utilisent l'eau de manière ouverte, c'est-à-dire de l'eau que l'on ne récupère pas. Je parle de ces fameuses tours que l'on voit sur les centrales nucléaires, d'où s'échappe un nuage de vapeur. C'est l'une des très rares industries en France où l'on a le droit d'utiliser l'eau de manière ouverte pour le refroidissement : on prend l'eau du fleuve, on la fait passer sur le circuit chaud, elle s'évapore et disparaît. Pour les centres de données, c'est interdit. Aux États-Unis, c'est une méthode de refroidissement très répandue, et donc beaucoup plus consommatrice d'eau. En France, globalement, les centres de données ne sont pas de gros consommateurs d'eau et utilisent une énergie largement décarbonée. Mais il faut des années pour obtenir les autorisations de construction. À cause de ces délais, on n'en construit pas, on en manque, et on est obligé de se déployer dans des pays voisins. Honnêtement, il est dommage aujourd'hui de devoir se déployer dans des pays où l'électricité est beaucoup plus carbonée et dépendante de l'approvisionnement en gaz, souvent russe, alors que nous avons l'électricité en France et que nous pourrions le faire ici.

Mme Cyrielle Chatelain, rapporteure. Combien de projets sont aujourd'hui en attente d'autorisation, à votre connaissance ?

M. Damien Lucas. De tête, au moins cinq. Mais la question n'est pas tant le nombre de projets que la puissance totale associée. Il s'agit d'au moins cinq projets de plus de 100 mégawatts chacun, ce qui représenterait quasiment un doublement de la capacité existante sur le territoire français. Cela correspond probablement au besoin actuel, mais ces projets sont en attente d'obtenir les fameuses autorisations d'exploiter, les études « quatre saisons », etc. Le délai est d'au moins deux ans, je pense.

M. le président Philippe Latombe. Nous serions preneurs si vous pouviez nous transmettre cette liste de cinq projets afin que nous puissions les examiner.

M. Damien Lucas. Nous vous enverrons ces détails par écrit.

M. Philippe Miltin. Je n'ai que peu de choses à ajouter à ce qu'ont dit MM. Klaba et Lucas. Aujourd'hui, nous utilisons des data centers extérieurs et nous multiplions nos fournisseurs. Le critère du 100 % décarboné est effectivement extrêmement important. L'urbanisme des nouvelles salles, avec l'arrivée de l'IA, est également clé. Octave l'a rappelé, il y a aujourd'hui peu de fournisseurs d'infrastructures. Nous travaillons avec Bull, qui va nous fournir nos infrastructures d'IA, car nous allons développer ce que nous appelons des « IA factories » en dehors du cloud. C'est un sujet majeur qui demande un refroidissement à eau de base, mais qui présente aussi des caractéristiques différentes. Il est évident que les centres de données décarbonés, optimisés avec refroidissement à eau, sont une nécessité. Il est tout aussi évident que nous n'en avons pas suffisamment en France et en Europe. C'est un sujet sur lequel nous sommes tous en contact avec les promoteurs. Le temps de mise en œuvre reste un enjeu majeur.

Enfin, sur la partie HDS, je suis tout à fait d'accord avec Damien Lucas : c'est un sujet pour les citoyens. Je pense toutefois que combiner HDS et SecNumCloud reste, pour les données de santé, un élément de sécurité indispensable.

M. le président Philippe Latombe. Cela me permet de poser une question, ce qui changera l'ordre des intervenants. Je plaisantais à peine avec l'affaire Mythos tout à l'heure, mais c'est un phénomène que nous observons. Nous avons vu la Réserve fédérale américaine convoquer les banquiers américains pour leur expliquer qu'ils pouvaient trouver des failles. La BCE a fait de même, semble-t-il, le week-end dernier. Nous voyons l'IA arriver avec des capacités particulières. Sur la cybersécurité, qui était un argument très mis en avant par certains promoteurs des solutions américaines, notamment de cloud, affirmant que c'est dans ces solutions que la sécurité était la plus forte, nous assistons à une forte concentration des entreprises de cybersécurité, avec notamment le rachat d'entreprises européennes par des acteurs américains. Y voyez-vous un risque de dépendance à venir pour votre activité ? Est-ce une tendance qu'il faut inverser ? Comment percevez-vous cette concentration du marché de la cybersécurité, notamment au profit de capacités américaines ?

M. Sébastien Lescop. Pour parler de l'affaire Mythos, ce qui a été découvert, de ce que j'ai compris, c'était principalement ce qu'on appelle des vulnérabilités, des J0, qui n'étaient pas corrigées. Il faut savoir que le référentiel SecNumCloud impose que toutes les mises à jour de sécurité soient réalisées dans les temps. L'Anssi s'en assure lors de ses audits ; cela fait partie des vérifications standards.

Deuxièmement, sur le fait qu'un partenaire puisse changer de pavillon, est-ce un risque ? Je pense que c'est surtout un risque pour la France et son économie. Pour le consommateur d'un fournisseur de cloud, le risque dépend de la manière dont ce dernier gère ses partenaires. Chez Cloud Temple, nous avons construit une couche logicielle d'abstraction qui permet de ne pas répercuter la technologie que nous utilisons sur le consommateur final. C'est-à-dire que demain, si nous sommes en désaccord stratégique ou financier avec un partenaire, ou s'il y a un rachat et que se produit un « effet Broadcom », nous sommes capables de garantir à nos clients un plan de continuité de service. C'est l'engagement que nous prenons auprès d'eux. Bien sûr, nous préférons ne pas avoir à lancer de tels chantiers s'ils n'apportent pas de valeur ajoutée à nos clients. Néanmoins, nous nous sommes déjà prémunis, dès la conception de la plateforme, pour pouvoir y faire face si besoin était.

M. Éric Haddad. Nous n'avons pas identifié de vulnérabilité ou de dépendance par rapport à ce type de menace, car nous développons tout en open source, en système ouvert. Nous maîtrisons complètement ce que nous développons. Il n'y a pas de licences à payer à des acteurs américains, en l'occurrence, jusqu'à présent.

M. le président Philippe Latombe. Vous n'utilisez absolument aucune solution de centre opérationnel de sécurité (SOC), de plan de reprise d'activité ou autre ?

M. Éric Haddad. Le SOC que nous avons est celui de La Poste. Mais pour notre plateforme, tout ce que nous utilisons, y compris pour les aspects de cybersécurité, est issu de l'open source.

M. le président Philippe Latombe. Y a-t-il un sujet que nous n'avons pas abordé et que vous voudriez évoquer ? C'est la question rituelle de fin. Je sais que vous suivez les auditions. Si des sujets émergent au cours des prochaines auditions et sur lesquels vous

souhaitez réagir, positivement ou négativement, n’hésitez pas à nous faire parvenir des contributions écrites.

Je précise, puisque cette audition est retransmise sur le site de l’Assemblée nationale, que vous faites partie des fournisseurs de cloud, mais que d’autres auraient pu être invités. Nous avons essayé de limiter le panel, ce qui ne signifie pas que vous êtes les seuls. C’était important de vous avoir, mais je préférais expliquer pourquoi vous étiez tous les cinq.

Merci en tout cas de votre présence. La séance est levée.

La séance s’achève à quinze heures cinquante.

———

Membres présents ou excusés

Présents. – Mme Cyrielle Chatelain, M. Philippe Latombe.