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

Mercredi
13 mai 2026
Séance de 15 heures

Compte rendu n° 44

SESSION ORDINAIRE DE 2025-2026

Présidence de
M. Philippe Latombe,
Président de la commission

ASSEMBLÉE NATIONALE

La séance est ouverte à quinze heures.

La commission entend, lors de sa table ronde réunissant des représentants en France des Gafam :

– Mme Corine de Bilbao, présidente de Microsoft France, et M. Philippe Limantour, directeur technologie et cybersécurité ;

– M. Sébastien Missoffe, directeur général de Google France et M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google Cloud ;

– M. Julien Lépine, représentant en France d'Amazon Web Services Europe, Moyen-Orient, Afrique (AWS EMEA), et M. Arnaud David, directeur des affaires publiques France et Union européenne de AWS.

M. le président Philippe Latombe. Madame, messieurs, je vous remercie de vous être rendus disponibles pour participer à cette table ronde réunissant les représentants en France des géants du numérique, les Gafam.

À eux trois, Amazon Web Services (AWS), Microsoft Azure et Google Cloud représentent 70 % du marché européen du *cloud*. Comment les données hébergées sont-elles protégées ? Comment sont-elles exploitées ?

Je vais vous laisser la parole pour un propos liminaire d'une dizaine de minutes chacun. Vous pourrez nous présenter vos entreprises respectives au niveau mondial et européen, ainsi que l'activité réalisée en France. Au préalable, je vous remercie de nous déclarer tout intérêt public ou privé de nature à influencer vos déclarations.

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 le serment de dire la vérité, toute la vérité, rien que la vérité.

(Mme Corine de Bilbao, M. Philippe Limantour, M. Sébastien Missoffe, M. Frédéric Geraud de Lescazes, M. Julien Lépine et M. Arnaud David prêtent successivement serment.)

Mme Corine de Bilbao, présidente de Microsoft France. Je vous remercie sincèrement de nous donner l'occasion de contribuer à vos travaux. Les questions que vous examinez sont légitimes, importantes et complexes. Des échanges comme celui-ci, avec la représentation nationale, nous permettent d'apporter des réponses factuelles et opérationnelles aux questions que les enjeux de souveraineté et le contexte géopolitique suscitent.

La réalité, c'est que ces questions se posent également avec nos clients. Elles ont conduit Microsoft à prendre des engagements concrets visant à renforcer la continuité des services, la protection des données et la résilience numérique en Europe. En tant que présidente de Microsoft France, que j'ai rejoint en 2021, je porte une attention constante à ces enjeux car, dans notre industrie, la confiance constitue un fondement essentiel.

Le numérique, comme toute chaîne de valeur stratégique, repose sur un ensemble d'interdépendances, des minerais critiques et infrastructures énergétiques jusqu'aux centres de données, aux capacités de calcul, aux modèles d'intelligence artificielle (IA), ou encore aux logiciels. Aussi l'enjeu réside-t-il dans l'organisation et la gouvernance de ces interdépendances, ainsi que dans les garanties concrètes apportées par les différents acteurs de cette chaîne pour les maîtriser.

Microsoft est présent en France depuis plus de quarante ans et compte près de 2 200 collaborateurs. Mais la réalité de notre présence ne se résume pas à nos effectifs : Microsoft est en effet un moteur de la filière des services informatiques et des logiciels, grâce à la constitution d'un écosystème de 10 500 partenaires, qui représentent 80 000 emplois répartis sur l'ensemble du territoire.

Notre modèle en France est avant tout un modèle de plateforme et de partenariat. Nous intervenons comme fournisseur de technologies avec une logique de collaboration, de complémentarité et de partage de valeur, sans nous substituer à nos clients. Aujourd'hui, pour 1 euro de solutions et de services facturés par Microsoft en France, les partenaires génèrent près de 6 euros de chiffre d'affaires. Cet effet multiplicateur illustre le rôle d'entraînement que peut jouer notre présence dans l'économie numérique française. Par exemple, s'agissant du secteur public, Microsoft ne répond pas directement aux procédures de passation des marchés publics : ce sont les revendeurs, intégrateurs et prestataires qui se positionnent sur ces consultations, dans le respect du droit de la commande publique.

Notre présence en France se traduit également par des investissements concrets. En 2024, nous avons annoncé un investissement de 4 milliards d'euros pour développer des infrastructures de *cloud* et d'intelligence artificielle de pointe, former un million de Français aux usages de l'IA et accompagner 2 500 start-up dans cette nouvelle économie.

J'en viens à un point important : le modèle de l'économie du *cloud*. Nos technologies ne sont jamais simplement posées sur étagère : elles doivent être intégrées, configurées et opérées pour répondre aux besoins de nos clients. Ce travail est, dans une très large mesure, réalisé par des acteurs français, dont de nombreuses PME.

Dans cette économie du *cloud*, Microsoft a depuis longtemps fait le choix de l'ouverture. Notre plateforme de *cloud* public Azure n'est pas une infrastructure propriétaire fermée. Nos clients peuvent choisir librement parmi un grand nombre d'options propriétaires ou *open source* pour les serveurs, les bases de données ou les réseaux. Ainsi, environ deux tiers des machines virtuelles de nos clients sur Azure exécutent Linux. Dans le domaine de l'IA, nous appliquons les mêmes principes : notre infrastructure Azure propose un catalogue de plus de 11 000 modèles comprenant des offres de Mistral, d'OpenAI ou l'ensemble des modèles *open source* d'Hugging Face.

La protection des données est au cœur de la relation de confiance avec nos clients. Elle repose sur des garanties concrètes, des contrats, des protections techniques et, lorsque c'est nécessaire, la capacité de défendre nos clients devant les tribunaux. Ainsi, Microsoft conteste systématiquement les demandes d'accès aux données de ses clients, en Europe comme dans le reste du monde.

Il me paraît important de rappeler ce que le Cloud Act permet et ce qu'il ne permet pas. Le Cloud Act n'autorise pas un accès automatique, massif ou non ciblé aux données des clients, bien au contraire : toute demande d'accès à des données de contenu nécessite

l'intervention d'un juge, sur la base d'une cause probable que les données demandées contiennent des preuves d'un crime grave et spécifique relevant de la juridiction américaine, par exemple un acte de terrorisme ou de pédocriminalité.

Microsoft n'accorde en aucun cas aux autorités un accès général ou illimité aux données de ses clients. L'entreprise ne communique ni les clés de chiffrement de ses clients, ni aucun moyen permettant de contourner les mécanismes de protection ; elle conteste toute demande imprécise, excessive ou en conflit avec le droit d'un autre pays. Je tiens également à préciser que Microsoft n'a jamais divulgué de données d'un client du secteur public français à des autorités étrangères, y compris américaines.

Ces garanties juridiques s'inscrivent dans une logique plus large de convergence entre États démocratiques en matière de protection des citoyens contre les crimes les plus graves. Ainsi, l'Union européenne a adopté en 2023 le règlement « e-evidence », qui permet à une autorité d'un État membre d'ordonner directement à un prestataire de *cloud* de produire ou de conserver des preuves électroniques, quel que soit le lieu où se trouvent les données.

Pour aller plus loin, j'évoquerai les engagements de Microsoft pour la protection des données de ses utilisateurs. Le règlement général sur la protection des données (RGPD) a constitué un jalon majeur, que nous avons choisi d'étendre au niveau mondial. Au-delà de ce cadre juridique, nous avons mis en place, en Europe, des garanties opérationnelles supplémentaires. Notre initiative EU Data Boundary (frontière européenne des données), finalisée en 2025, vise à ce que les données des clients soient localisées et traitées au sein de l'Union européenne et de l'Association européenne de libre-échange (AELE). Enfin, en cohérence avec ce modèle, Microsoft s'engage contractuellement à ne pas utiliser les données de ses clients entreprises et du secteur public à des fins publicitaires, ni à en tirer des informations à des fins commerciales. Ce n'est pas notre modèle économique.

J'en viens à la souveraineté. Les exigences en matière de souveraineté opérationnelle varient d'un pays à l'autre, et même d'un client à l'autre. Nous nous conformons systématiquement à la législation des États dans lesquels nous opérons. Tout d'abord, les contrats conclus avec nos clients européens prévoient expressément notre engagement à respecter le droit de l'Union européenne, dans tous les cas et sans exception. Ensuite, depuis près d'un an, nos offres de *cloud* proposent des fonctionnalités renforcées de protection, de confidentialité des données et de chiffrement permettant à nos clients de déployer nos solutions dans des configurations adaptées à leurs contraintes opérationnelles, y compris dans des environnements totalement déconnectés et pour les modèles d'IA.

La confiance passe aussi par des dispositifs concrets de transparence et de coopération avec les autorités publiques. En France, cette coopération est engagée depuis le début des années 2000 avec l'Agence nationale de la sécurité des systèmes d'information (Anssi). Elle se traduit par un partage d'informations sur les menaces, des échanges techniques avec nos équipes d'ingénierie et un accès sécurisé, en lecture seule, à une sélection de codes sources.

De plus, la France s'est dotée d'un cadre protecteur pour les données les plus sensibles, matérialisé par la qualification SecNumCloud. C'est dans ce cadre qu'Orange et Capgemini ont conjointement créé Bleu, un *cloud* français sécurisé opéré par une entité de droit français totalement indépendante de Microsoft. Nous sommes seulement un fournisseur technologique, sans lien capitalistique ni contrôle opérationnel. Les services *cloud* de Bleu sont physiquement déconnectés du *cloud* public de Microsoft.

Enfin, en partenariat avec plusieurs acteurs européens, nous développons des dispositifs de continuité pour assurer la disponibilité des services essentiels dans toutes les situations.

Je souhaite enfin revenir sur le sujet majeur de la cybersécurité. C'est une dimension centrale de toute la réflexion sur les dépendances numériques. D'après notre rapport annuel de cybersécurité, la France se classe au quatrième rang des pays les plus attaqués en Europe. Les services publics critiques sont particulièrement ciblés par les cybercriminels. La lutte contre la cybercriminalité repose sur une coopération étroite entre les acteurs publics et privés. Microsoft partage avec la France des informations détaillées sur l'état de la menace afin de contribuer à la protection des infrastructures critiques. La résilience des services numériques passe aussi par la capacité à protéger physiquement les infrastructures. Ainsi, en 2022, nous avons pu alerter les autorités ukrainiennes des risques de destruction de leurs infrastructures informatiques et organiser le transfert de leurs données et services critiques vers des *data centers* situés en Europe.

Aucun État ni aucune entité ne pourra maîtriser seul l'intégralité de la chaîne de valeur de l'intelligence artificielle. Celle-ci est trop vaste, trop intensive en capital, en talents, en recherche, en infrastructures et en cybersécurité pour être concentrée durablement dans un seul pays. Cela signifie que la chaîne de valeur de l'IA reposera sur des interdépendances fortes, à la fois technologiques, industrielles et géographiques. La France dispose à cet égard de nombreux atouts : d'excellentes entreprises dans le développement de modèles tels que Mistral AI, des acteurs innovants dans les applications d'IA, des équipes de recherche de premier plan, des compétences fortes dans l'évaluation, la cybersécurité et l'intégration de ces technologies dans l'économie. C'est peut-être dans cet esprit d'ouverture que nous pourrons essayer de contribuer utilement aux travaux que vous menez sur les questions de dépendance, de résilience et de capacité d'action.

M. Sébastien Missoffe, directeur général de Google France. Nous vous remercions de votre invitation. Nous sommes pleinement conscients de l'importance du travail de votre commission d'enquête, qui traite d'un sujet important, au cœur de vos préoccupations et de celles des Françaises et des Français, dans un contexte géopolitique source de tensions et d'inquiétudes très légitimes.

Je vais vous partager brièvement le point de vue de Google. Quant à mon collègue Frédéric Geraud de Lescazes, il répondra à vos questions concernant spécifiquement le *cloud* et vous présentera les solutions pratiques et responsables sur lesquelles nous travaillons avec nos partenaires locaux, comme Thales pour la partie informatique en nuage.

Google a ouvert son premier bureau à Paris en 2004. Quand j'en ai pris la direction, en 2017, il y avait environ 700 employés ; nous sommes aujourd'hui 1 350, soit quasiment le double.

La mission de Google est de rendre l'information accessible et utile pour tous. Nous la prenons très au sérieux, car elle est au cœur de notre engagement. Nos collaborateurs représentent la majorité des activités clés de l'entreprise : marketing, *cloud*, ingénierie, recherche, partenariat. Nos équipes accompagnent nos clients et nos utilisateurs pour leur permettre de tirer pleinement parti des technologies numériques.

C'est dans ce cadre que nous avons développé des partenariats étroits avec des entreprises françaises, pour contribuer à leur compétitivité. Nous travaillons avec de grands groupes industriels français, par exemple sur des jumeaux numériques, afin d'améliorer la

sécurité de leurs produits ou de lancer des produits plus rapidement, contribuant ainsi à leur compétitivité. Nous travaillons également avec des start-up, pour les aider à se développer à l'international, contribuer à leur compétitivité et développer des champions internationaux depuis la France. Nous avons enfin des activités de recherche sur l'intelligence artificielle : en février 2024, nous avons ainsi ouvert un nouveau centre d'intelligence artificielle à Paris, comptant un peu plus de 300 personnes et développant nombre de collaborations, dont l'une avec l'Institut Curie sur des recherches de prédiction du cancer.

Les débats actuels concernent plus spécifiquement Google Cloud Platform, connue sous le nom de GCP, qui est l'un des derniers entrants sur le marché de l'informatique en nuage. Selon le dernier rapport de l'Autorité de la concurrence, que vous avez pris en référence pour vos travaux, GCP est le cinquième acteur du marché de l'informatique en nuage en France, avec moins de 10 % de parts de marché, derrière AWS, Microsoft, Orange Business et OVH.

Les trois acteurs ici présents représentent trois choix technologiques, trois positions de marché et trois stratégies différentes. Compte tenu de notre position de marché, nous sommes toujours favorables à toute action permettant de fluidifier et d'ouvrir ce marché en expansion, notamment en France, où l'adoption des technologies en nuage se fait plus lentement que dans le reste de l'Union européenne.

Côté secteur public, vous ne trouverez pas trace de Google dans le top 10 des fournisseurs de l'État – notamment dans les marchés de l'Union des groupements d'achats publics (Ugap) –, selon les chiffres de la direction interministérielle du numérique (Dinum). Ayant très peu de parts de marché dans le secteur public, notre action n'est pas guidée par la nécessité de les conserver : cela nous permet d'avoir une approche différente.

Google croit en un *cloud* au service de l'économie française, qui tient sa promesse initiale – une promesse d'ouverture, de sécurité, d'élasticité, de simplicité, et surtout une grande liberté de choix pour le client, notamment pour tester de nouvelles fonctionnalités et innovations. Google se différencie aussi par des services fondés sur des technologies *open source*. Nous sommes connus pour cela.

S'agissant de la sécurité des données, qui constitue l'un des principaux enjeux, nous offrons déjà à tous nos clients la capacité de choisir librement le type de contrôle requis et la localisation de leurs données.

Enfin, nos ingénieurs travaillent constamment à l'amélioration de l'efficacité énergétique de nos solutions : c'est nécessaire du point de vue de leur impact environnemental, mais cela relève aussi de notre intérêt économique. En 2024, nos centres de données ont fourni six fois plus de puissance de calcul par unité d'électricité que cinq ans auparavant. Nos centres de données ont utilisé 84 % moins d'énergie que la moyenne du secteur. Nous investissons aussi dans des énergies propres. Ces dernières années, Google a ainsi signé des accords en Europe portant sur plus de 4,5 gigawatts, notamment au travers de partenariats avec Engie.

Nous produisons enfin nos propres puces, dont chaque génération – nous en sommes à la huitième – apporte des gains considérables. Vous l'aurez compris, le mouvement d'amélioration est continu.

Je laisse Frédéric Geraud de Lescazes vous présenter plus en détail Google Cloud.

M. Frédéric Geraud de Lescazes, directeur des affaires publiques de Google Cloud. Le sujet de nos dépendances et vulnérabilités numériques n'est pas seulement une question technique : il concerne à la fois la sécurité nationale, la prospérité économique et la compétitivité, notamment au travers de la liberté de choix. Tout le monde a des dépendances, Google comme les autres.

Il n'y a, de notre point de vue, qu'un seul véritable sujet de dépendance sur le marché du *cloud* : c'est la monoculture, frein à l'adoption du *multicloud* et frein à plus d'interopérabilité, de sécurité et de portabilité, autrement dit de liberté de choix de son fournisseur. Cette monoculture est contrainte et souvent déloyale ; nombre de vos auditions ont déjà fortement souligné ce sujet. Nous dénonçons le *vendor lock-in*, c'est-à-dire des pratiques d'enfermement juridique des clients, issues des pratiques déloyales des acteurs présents avant l'arrivée de l'internet grand public. Nous en souffrons, comme tous les autres acteurs du marché. Il est important que la commission sache que ce combat, vieux de plus de dix ans, fut d'abord celui d'OVH et de l'ensemble des fournisseurs de *cloud* européens de toutes tailles, rassemblés au sein de l'organisation CISPE (Cloud Infrastructure Service Providers Europe). Puis ce fut celui du Cigref, le Club informatique des grandes entreprises françaises, qui rassemble leurs directions des systèmes d'information (DSI), notamment lors des débats sur la loi visant à sécuriser et à réguler l'espace numérique (loi Sren). Aucun acteur, petit, moyen ou grand, ne pourra grandir sur ce marché tant que perdureront ces pratiques anticoncurrentielles. Un client doit pouvoir quitter son fournisseur ; sinon, le jeu est faussé. L'autorité de la concurrence britannique, dont les travaux sont exemplaires, s'est d'ailleurs emparée de ce sujet.

Le deuxième mot-clé de cette commission est la vulnérabilité ; elle a pour pendant la résilience. La publication de la doctrine « Cloud au centre », en 2021, et le primat du SecNumCloud nous ont convaincus que, sur le segment des données sensibles, nous ne pourrions tout simplement plus exister. En effet, de nationalité et de capital, nous sommes américains. Par construction, le SecNumCloud ne peut pas être pour nous. Cela ne nous fait pas plaisir d'être exclus du marché des données sensibles, mais nous en avons pris acte, avec deux convictions fortes.

Notre première conviction, c'est que nous devons respecter nos utilisateurs. Eux seuls sont à même de définir leurs besoins, de savoir ce qu'ils veulent. À nous, Google Cloud, de trouver une solution pour leur répondre. Autrement dit, Google Cloud offrira toujours le choix.

Notre deuxième conviction, c'est que la France, comme n'importe quel autre pays, ne doit pas avoir à choisir entre l'innovation de pointe et son autonomie stratégique – ce que certains nomment souveraineté. Chez Google Cloud, nous pensons que la dépendance n'est pas une fatalité. Nous proposons déjà des solutions fonctionnelles entièrement déconnectées, avec de l'intelligence artificielle ; ces solutions « dans une bulle d'air » ont beaucoup de succès, notamment dans la défense et les services financiers.

Nous avons aussi apporté nos technologies à une autre offre du marché qui répond aux problèmes de vulnérabilité et de protection face aux lois extraterritoriales. Vous la connaissez sous le nom commercial de Premi3ns ; elle est opérée et contrôlée par une coentreprise nommée administrativement Thales Cloud Sécurisé, que vous connaissez sous la marque S3NS. Thales est le seul maître à bord de S3NS : Google Cloud ne dispose que d'un siège d'observateur, sans droit de vote ni droit de veto.

Cette offre Premi3ns est qualifiée SecNumCloud depuis décembre dernier, sur trois segments : l'infrastructure, les plateformes et les containers. Il n'y a pas la partie logicielle à la

demande, dite SaaS (*Software as a Service*), où se situent notamment les suites collaboratives. Une place de marché SaaS se crée sous nos yeux, sur S3NS, avec de belles synergies en cours. D'ailleurs, le plus gros fournisseur de services SaaS européen est allemand : SAP ne s'y est pas trompé, il recourt à S3NS. Il existe donc déjà plusieurs solutions au problème de la vulnérabilité, grâce à la vision anticipatrice et au travail rigoureux et méticuleux engagé il y a près de quinze ans par les équipes de l'Anssi.

S3NS a pris le meilleur des deux mondes. Il s'agit de la seule offre SecNumCloud hyper-échelle, la seule offre qualifiée avec un catalogue de services bientôt aussi large qu'un *hyperscaler*, dont des solutions d'intelligence artificielle. C'est son avantage le plus connu, mais S3NS est également déjà résilient à l'arrivée du post-quantique, car Thales est un champion mondial des algorithmes résilients au quantique.

S3NS est un avantage stratégique à la main de Thales, dont le premier actionnaire est l'État. Il ne cache d'ailleurs pas son ambition de devenir le premier *hyperscaler* européen. Cela fait vingt-cinq ans que l'on souhaite avoir un champion français de taille européenne : nous y sommes, et ce champion français et européen capable de concurrencer les *hyperscalers* ne vient pas de l'informatique ni des télécoms, mais de la défense.

L'Anssi a dit qu'il n'existait pas d'offre 100 % française. L'Agence a aussi dit qu'elle ne faisait pas de politique industrielle – mais elle peut tout de même l'orienter… Vous avez depuis décembre dernier un champion européen de la défense et de la cybersécurité, avec des équipes massives d'ingénieurs de haute qualité en France, avec ses propres infrastructures, ses propres centres de données, ses propres lignes de production de matériel… Thales recrute beaucoup en France. Il apprend à faire du *cloud* et de l'intelligence artificielle avec Google. C'est une aventure industrielle où seul Thales décide.

S3NS profite également de la recherche et développement (R&D) de Google Cloud sans en supporter le coût, qui se chiffre en milliards. Le directeur général de l'Anssi a souligné ce bénéfice lors de son audition, d'abord pour Thales, mais probablement aussi pour de nombreux autres services de l'État. Il a fallu cinq ans – c'est long ! – avant de pouvoir sortir une solution fonctionnelle. Les ingénieurs de Thales ont accompli un travail titanesque : ils ont fait qualifier une trentaine de services et ont reçu la qualification SecNumCloud pour trois ans, sans aucune réserve de l'Anssi. Vraiment, c'est un travail remarquable des équipes Thales et S3NS !

Nous avons pris le risque de transmettre nos technologies et nos savoir-faire à S3NS, qui est, dans les faits, un nouvel offreur de services *cloud*, donc un concurrent des *hyperscalers*. Cela a pris cinq ans, car les référentiels de l'Anssi ne sont pas légers. L'Anssi a utilisé devant vous l'expression « dispositif lourd » : c'est un doux euphémisme ! Nous avons pu observer de près le parcours du combattant de S3NS pour obtenir la qualification. Il faut bien se rendre compte de la prouesse technologique. S3NS est unique au monde, car le SecNumCloud est unique au monde. S3NS, qui reçoit depuis peu des appels du monde entier, constitue un avantage stratégique pour la France et l'Europe. D'ailleurs, la Commission européenne a déjà retenu cette solution pour ses propres besoins sensibles, au sein d'un consortium.

Le risque n'est pas d'utiliser les meilleures technologies mondiales, mais de s'en priver. Pour nous, le *cloud* est d'abord une question de liberté de choix, notamment de choix d'architecture logicielle dite ouverte, mais aussi de gouvernance et des conditions juridiques vous permettant de quitter votre fournisseur – bref, de ne pas être enfermé. Encore faut-il trouver le bon partenaire, qui accepte de le faire selon vos conditions et de jouer selon vos règles, y compris celle de vous laisser partir.

M. Julien Lépine, représentant en France d'Amazon Web Services (AWS) Europe, Moyen-Orient, Afrique. Avant de partager nos observations, permettez-moi de vous présenter brièvement qui nous sommes et ce que nous faisons. Amazon Web Services, que je désignerai par l'acronyme AWS, est une entreprise fournissant des services d'infrastructure *cloud* aux organisations publiques et privées pour les aider à innover tout en protégeant leurs données.

Cette année, nous célébrons nos vingt ans, et l'année prochaine, les dix ans de nos premiers centres de données en France. AWS compte aujourd'hui près de 900 salariés sur le territoire français. Le métier d'AWS est de fournir des ressources informatiques à la demande, avec une tarification à l'usage. Concrètement, nos clients disposent d'un large choix technologique de plus de 200 services, d'une centaine de modèles d'intelligence artificielle, dont ceux de Mistral AI, et de dizaines de milliers de solutions logicielles partenaires au travers de notre place de marché. Ils n'utilisent que ce dont ils ont besoin, quand ils en ont besoin.

J'ai eu la chance de rejoindre AWS en 2012, alors que l'entreprise commençait son implantation en France. En tant qu'ingénieur formé en France, j'ai saisi l'opportunité de faire bénéficier à toute la filière technologique française des outils, de la sécurité et de l'innovation apportés par le *cloud*.

Je souhaite partager avec vous trois convictions qui guident notre action en France.

Premièrement, nous sommes fiers de contribuer au développement des entreprises françaises de toutes tailles. Depuis vingt ans, notre mission est de donner aux PME les mêmes moyens technologiques que les grands groupes pour innover et se développer.

Deuxièmement, nous sommes convaincus que le *cloud* AWS permet d'offrir à tous les clients français un niveau de sécurité des données qu'ils ne pourraient atteindre seuls. Face à l'explosion des cybermenaces, le *cloud* constitue la meilleure réponse pour protéger les données des organisations publiques et privées.

Troisièmement, nous pensons que les entreprises françaises ne devraient pas avoir à choisir entre innovation et souveraineté numérique : il faut garantir les deux. C'est précisément ce que nous permettons. Depuis sa création, AWS a accompagné des champions français et européens qui sont devenus des leaders mondiaux, que ce soit dans le transport, la gestion de flux financiers ou la recherche. Ces entreprises ont créé des milliers d'emplois en France, développé des innovations majeures, généré des milliards d'euros de recettes, réinvesti dans l'économie française et, surtout, changé la vie quotidienne et professionnelle des Français.

Lorsque nous avons ouvert nos infrastructures en France, en 2017, nous avons établi un plan d'investissement sur quinze ans, d'un montant de 6 milliards d'euros, pour soutenir la compétitivité des entreprises françaises. La majorité de ces investissements irriguent directement le tissu économique français – construction, raccordement, installation et exploitation partagée de centres de données en partenariat avec des entreprises locales.

La semaine dernière, Amazon a annoncé son plus grand investissement jamais réalisé en France : plus de 15 milliards d'euros sur trois ans, créant 7 000 emplois permanents. Les investissements d'AWS s'inscrivent naturellement dans l'ancrage d'Amazon en France, toutes activités confondues – logistique, distribution, médias et technologies. Depuis 2010, plus de 30 milliards d'euros ont été investis et plus de 25 000 emplois permanents ont été créés sur le territoire, au service de l'économie française.

Notre modèle d'affaires repose sur des centaines de partenaires qui cocréent de la valeur au plus près de nos clients, tels que Devoteam, Sopra Steria, Atos Eviden ou encore Kiiro. Ces partenaires conçoivent les solutions, accompagnent les transformations numériques et créent de l'emploi sur le territoire.

Comme toute entreprise technologique de taille mondiale, AWS s'appuie sur une chaîne d'approvisionnement globale. À ce titre, nous développons et utilisons des technologies conçues en Europe, tout en les diffusant dans le monde entier. Certaines de nos technologies de pointe, comme Nitro, notre système de sécurité matérielle garantissant qu'aucun opérateur d'AWS ne peut accéder aux données des clients, sont conçues dans nos centres de R&D en Europe, notamment en Allemagne. Les serveurs équipant nos centres de données en Europe sont assemblés, réparés et recyclés en Irlande aujourd'hui, et le seront bientôt en Espagne. Notre puissance de calcul repose sur des fournisseurs de solutions de semi-conducteurs avancées, comme celles de STMicroelectronics, leader franco-européen avec lequel nous venons de conclure un partenariat stratégique.

Cela reflète une réalité fondamentale : la chaîne de valeur technologique est mondiale et interdépendante. Les fournisseurs de *cloud* et d'IA dépendent de fournisseurs de puces informatiques, de routeurs, de serveurs, de disques situés en Europe et en dehors. Ce qui importe, c'est d'encourager l'utilisation des technologies innovantes tout en préservant la liberté de choix technologique, celle qui permet à chaque organisation de sélectionner les solutions les plus adaptées à ses besoins.

Ces investissements et ces partenariats visent précisément à répondre aux vulnérabilités que votre commission examine. La plus urgente, de loin, est la cybersécurité. Le paysage des menaces n'a jamais été aussi critique, et les PME en restent les premières victimes. Les organisations qui migrent vers le *cloud* bénéficient d'un niveau de protection qu'elles ne pourraient atteindre seules : chiffrement avancé, détection et correction automatisée des anomalies, redondances permettant la restauration rapide des systèmes en cas d'attaque.

La sécurité est notre priorité. AWS protège des millions de clients actifs dans le monde. Notre infrastructure de sécurité analyse chaque jour 400 000 milliards de flux réseau et détecte 182 000 nouveaux domaines malveillants. En 2025, nous avons bloqué plus de 300 millions de tentatives de rançongiciels. C'est le traitement de la cybersécurité à l'échelle qui rend le *cloud* plus sûr qu'une infrastructure isolée.

Le principe fondamental de la résilience est de ne pas concentrer les données en un seul endroit. Nos centres de données sont répartis sur trente-neuf zones géographiques, et nos clients choisissent où ils souhaitent stocker leurs données. C'est cette distribution qui protège contre les menaces modernes, qu'elles soient géopolitiques, environnementales ou techniques. Ainsi, en février 2022, dans les heures qui ont suivi l'invasion de l'Ukraine, nous avons aidé le gouvernement de ce pays à sécuriser plus de dix pétaoctets de quarante-deux autorités gouvernementales, pour ne plus dépendre de centres de données isolés et menacés de destruction. L'architecture *cloud* a permis de mettre ces données hors de portée des frappes, en quelques heures ; le gouvernement pouvait ainsi continuer d'exercer ses missions les plus critiques.

Le *cloud* offre le meilleur niveau de protection pour les données. Je l'ai dit, les organisations publiques et privées peuvent bénéficier d'un niveau de protection supérieur en ayant recours au *cloud*, leur permettant de prévenir, de détecter et de remédier aux cyberattaques.

Le *cloud* d'AWS répond déjà aux besoins de la majorité de ces organisations, grâce à son infrastructure située en France. Pour celles qui sont soumises à des exigences de souveraineté supplémentaires, notamment en matière de localisation des données, d'autonomie opérationnelle ou de conformité réglementaire, nous avons lancé en janvier dernier le *cloud* souverain européen d'AWS. Il s'agit d'un nouveau *cloud* indépendant pour l'Europe, physiquement et opérationnellement isolé des autres infrastructures AWS, qui propose plus de 100 services *cloud* innovants, y compris d'intelligence artificielle. Tout ce qui est nécessaire au fonctionnement du *cloud* souverain européen d'AWS se trouve dans l'Union européenne : les talents, la technologie, les infrastructures et la gouvernance. Aucun contrôle opérationnel ne s'exerce depuis l'extérieur des frontières européennes. Les opérations quotidiennes telles que l'accès aux centres de données, le support technique et le service client sont assurées exclusivement par du personnel européen. Ce nouveau *cloud* d'AWS bénéficie d'une autonomie de fonctionnement, même si l'Europe devait être coupée du reste du monde.

En définitive, l'enjeu n'est pas de choisir entre souveraineté et innovation, mais de garantir les deux. Aujourd'hui, le *cloud* ne représente que 20 % de l'informatique des organisations publiques et privées. Cela signifie que 80 % des systèmes d'information restent sur des infrastructures traditionnelles, souvent moins sécurisées, moins résilientes ou moins agiles. Il est donc impératif d'encourager l'adoption du *cloud* par les organisations publiques et privées pour leur permettre d'innover plus rapidement, de se transformer et de rivaliser à l'échelle mondiale tout en protégeant leurs données contre les menaces. C'est en migrant vers le *cloud* que les organisations accèdent aux meilleurs outils de cybersécurité, et c'est en garantissant la sécurité et la souveraineté que l'on crée la confiance nécessaire à cette adoption. C'est pour relever ce double défi qu'AWS s'engage en France par ses investissements à long terme, sa technologie, ses partenaires sur le territoire et des solutions adaptées aux exigences les plus strictes.

M. le président Philippe Latombe. Avant d'en venir au fond, j'aimerais vous poser quelques questions formelles.

Un salarié de Microsoft a été licencié quelques jours après son audition devant une commission d'enquête du Sénat, pour laquelle il avait prêté serment. Aussi, quelle valeur accordez-vous au fait de prêter serment ? Je tiens à vous rappeler que vous vous êtes engagés à dire la vérité, même si cela vous expose au risque de perdre votre emploi.

Interrogé sur l'une des réponses apportées par ledit salarié à la commission d'enquête, le patron de Microsoft a déclaré qu'il s'agissait d'une « réponse stupide à une question stupide ». Les parlementaires français sont-ils moins bons ou meilleurs que les Américains ?

Mme Corine de Bilbao. Pour être très claire, je précise que le départ de M. Anton Carniaux, car je suppose que c'est de lui que vous parlez, n'a strictement rien à voir avec son audition par une commission d'enquête du Sénat. Il n'y a absolument aucun lien.

Les sujets étudiés par votre commission sont extrêmement importants pour nous. J'en veux pour preuve l'ensemble des annonces et des investissements faits au niveau européen, que ce soit en matière de protection des données, de cybersécurité ou d'accompagnement des États. Je pense en particulier aux engagements contractuels que nous avons pris en matière de résilience, notamment envers les administrations publiques et les acteurs d'infrastructures et de services critiques.

Les enjeux relatifs au Cloud Act ont gagné en importance et, au cours des derniers mois, nos clients nous ont systématiquement posé des questions à ce sujet. J'ai rappelé dans mon propos liminaire ce que le Cloud Act permettait et ce qu'il ne permettait pas. Nous étudions chaque demande, qui doit être émise par un juge, avec des juristes américains et européens. Nous respectons le droit international, notamment la *comity* qui met en balance les droits des différents États. Les demandes sont transmises aux clients, et nous avons pris l'engagement contractuel de contester toute requête devant les tribunaux. Je tenais à le rappeler, car cela me semble important pour vos travaux.

M. le président Philippe Latombe. Vous ne répondez pas tout à fait à ma question, que je vous reposerai donc de manière différente. La sortie de votre président nous pousse à nous demander, nous, parlementaires français, si nos questions sont stupides. Je ne parle pas du Cloud Act, mais de la section 702 du Foreign Intelligence Surveillance Act (Fisa). Donnez-vous, oui ou non, des informations aux agences fédérales qui vous les demandent à ce titre ?

J'ai d'autres questions, auxquelles j'aimerais que chacune des entreprises me réponde par oui ou non.

Marco Rubio a envoyé un câble diplomatique indiquant qu'il fallait s'opposer à toute tentative de réglementation européenne, car elle constituait un problème pour les entreprises, notamment technologiques. Appliquez-vous ce câble diplomatique ? Faites-vous des opérations de lobbying contre la réglementation européenne ?

Enfin, le président Trump a demandé qu'il n'y ait plus de charte de diversité dans les entreprises américaines et a rappelé cette injonction à certaines entreprises françaises et européennes implantées aux États-Unis. Appliquez-vous la réglementation américaine, ou bien la réglementation européenne et française ? Désobéissez-vous au président Trump et à vos patrons, qui ont accepté de ne plus appliquer de telles chartes ?

M. Julien Lépine. Quelle valeur a notre parole ? Je peux parler en mon nom propre, et je me sens tout à fait soutenu par mon entreprise pour répondre à vos questions, qui sont pertinentes et légitimes.

La souveraineté est un enjeu vital pour la France, et nos entreprises l'ont bien compris. C'est l'un des fondamentaux de la création de notre plateforme et l'une des raisons pour laquelle nous agissons, en particulier en apportant des réponses technologiques sur lesquelles nous reviendrons. Se posent aussi des questions de process et de gouvernance. En tout cas, c'est la notion de souveraineté qui nous a guidés, ces vingt dernières années, dans la création d'infrastructures allant jusqu'à un *cloud* souverain européen.

Pour ce qui concerne le Fisa, je laisserai mon collègue Arnaud David vous répondre.

J'en viens à la diversité. Amazon, de manière générale, est une entreprise qui travaille avec des clients établis dans l'ensemble des pays : ils représentent toutes les religions, toutes les origines, toutes les manières de travailler. On ne peut pas se permettre d'avoir une entreprise qui ne s'adresse pas à ses clients. L'obsession client est une des valeurs fondamentales d'Amazon : si notre entreprise ne reflète pas la diversité de ses clients, nous ne pourrons pas les comprendre ni répondre à leurs demandes.

Pour la France, nous travaillons sur un ensemble d'initiatives. Nous publions, comme l'exige le droit français, un *gender equality index*. Nous menons aussi beaucoup d'activités en

faveur de la diversité. La succursale que je représente est une entreprise européenne, dont les politiques et les manières de travailler sont européennes.

M. le président Philippe Latombe. Sur le câble diplomatique de M. Rubio, est-ce vous qui répondez, ou bien votre collègue ?

M. Arnaud David, directeur des affaires publiques d'AWS pour la France et l'Union européenne. Je commencerai par votre dernière question. Nous publions de manière semi-annuelle des rapports de transparence, que je serai ravi de vous communiquer, sur les demandes qui nous sont adressées. À la fin de chacun de ces rapports, nous donnons une indication très factuelle : aucune demande adressée à AWS n'a été suivie d'une transmission au gouvernement américain de données appartenant à des entreprises ou des gouvernements situés hors des États-Unis. Si nous indiquons cela aussi clairement dans le rapport, c'est notamment parce qu'il existe un principe sous-jacent à de nombreuses lois auxquelles vous faites référence : on ne peut communiquer des données sur une base légale qu'à partir du moment où on peut techniquement y avoir accès. Or nous utilisons un certain nombre de technologies qui ne permettent pas d'accéder aux données des clients.

M. le président Philippe Latombe. Intégrez-vous dans vos rapports les demandes assorties d'une demande de secret de la part des agences fédérales ?

M. Arnaud David. Oui, il s'agit de tout type de demandes.

M. le président Philippe Latombe. Le câble de Marco Rubio appelle à s'opposer à toute tentative de nouvelle réglementation européenne, voire à combattre les dispositions existantes, comme le RGPD. L'appliquez-vous ?

M. Arnaud David. Depuis longtemps, nous contribuons à des travaux dans plusieurs pays européens et à l'échelon européen en général. Ils démontrent que nous avons mis en place des mécanismes très avancés, notamment en matière de protection des données, en collaboration avec beaucoup d'entreprises du secteur. Je pense au code de protection des données dans le *cloud*, qui a été, à ma connaissance, l'un des deux seuls codes validés par les autorités de protection des données des vingt-sept États membres. Nous avons récemment collaboré avec le Bureau européen de l'IA autour du premier code de bonnes pratiques pour la mise en œuvre de l'AI Act.

De manière générale, nous soutenons les réglementations européennes dès lors qu'elles sont basées sur une approche par les risques, ce qui est le cas du RGPD ou de l'AI Act, dont c'est même l'un des principes fondateurs, et qu'elles garantissent la possibilité pour nos clients d'innover.

M. Frédéric Geraud de Lescazes. Nous respectons les législateurs, qu'il s'agisse des parlementaires présents dans cette salle ou de ceux qui siègent partout ailleurs dans le monde, et nous venons devant eux pour dire la vérité.

S'agissant du câble diplomatique de Marco Rubio, nous sommes un acteur économique, non des agents gouvernementaux. Nous faisons avancer nos sujets.

S'agissant du lobbying, de l'influence et de la représentation d'intérêts, nos activités sont déclarées – en France, auprès de la Haute Autorité pour la transparence de la vie publique (HATVP), mais aussi à l'échelle européenne. L'activité de représentation des intérêts d'un acteur privé consiste à faire valoir ses arguments pour éclairer le débat quand une loi ou un

règlement sont élaborés. C'est en toute transparence que nous demandons des rendez-vous. Nos déclarations font l'objet de contrôles. Parmi les informations disponibles figurent notamment la taille du budget et les effectifs que nous dédions aux affaires publiques ; les sujets que nous abordons et les positions que nous défendons sont détaillés, ligne par ligne, action par action.

J'en viens au Fisa. Comme vous l'avez vous-même souligné, monsieur le président, le cadre réglementaire américain ne nous permet pas, à nous, entreprise américaine, de communiquer sur ces éléments. Vous trouverez dans notre rapport de transparence des fourchettes assez vagues, indiquant un ordre de grandeur allant de 0 à 500. Les équipes françaises n'ont pas connaissance d'éléments plus précis.

Sur la question de la diversité, nous n'avons absolument pas modifié nos engagements, notamment le soutien à certaines actions et initiatives, car nous pensons que notre diversité est une force.

Mme Corine de Bilbao. Je confirme ce qu'ont dit les autres entreprises : nous parlons en toute transparence sur l'ensemble des sujets.

Pour ce qui concerne le Cloud Act et le Fisa, nous pourrons vous transmettre notre rapport de transparence, qui recense l'ensemble des demandes émanant des juges. À cela s'ajoutent les réglementations françaises ou européennes, comme le règlement « e-evidence », qui concernent les demandes relatives à la criminalité et la cybercriminalité. Nous n'avons jamais communiqué de données issues des administrations publiques européennes. Par ailleurs, nous nous sommes engagés contractuellement à contester systématiquement les demandes devant les tribunaux, qu'elles relèvent du Cloud Act ou du Fisa. Je ne suis pas une spécialiste, mais nous vous communiquerons des éléments à ce sujet.

S'agissant de la réglementation européenne, nous avons adopté le RGPD dès le début, et nous avons même étendu son application au niveau mondial. Bien évidemment, en tant qu'entreprise mondiale, nous nous conformons aux réglementations de chacun des pays où nous sommes présents, et nous contribuons aux discussions à leur sujet.

Enfin, la diversité fait partie des valeurs de Microsoft. Permettre à chacun de réaliser ses ambitions fait partie de nos missions. Nos programmes de diversité sont toujours très dynamiques. En France, par exemple, nous avons six programmes portant notamment sur le genre, le handicap, l'âge et les origines. Bien évidemment, nous nous conformons à l'index de l'égalité et publions les rapports qui y sont associés. J'insiste sur ce point : la diversité fait partie des missions et des valeurs de notre entreprise, et cela ne change pas en fonction des gouvernements.

M. le président Philippe Latombe. Je note tout d'abord que vous n'appliquez pas les décisions américaines concernant la diversité. Cela me rassure, même si je ne vois pas comment il est possible, pour des entreprises telles que les vôtres, d'agir en ce sens. Mais nous allons regarder cela de plus près.

Je note ensuite, s'agissant du Fisa, une hétérogénéité de vos modes de fonctionnement : cela va de fourchettes très vagues, tenant compte du secret, à des informations à l'unité près ou presque.

Mme Cyrielle Chatelain, rapporteure. Vous avez apporté toutes les nuances nécessaires sur ce sujet complexe des demandes, qui comporte un volet juridique et un volet technique. Du point de vue juridique, tout d'abord, vous l'avez souligné, les demandes émises

dans le cadre du Cloud Act sont soumises à certaines conditions. Toutefois, les outils juridiques prévus dans le cadre de la lutte contre le terrorisme sont utilisés pour sanctionner des juges de la Cour pénale internationale (CPI). Ma première question sera simple : si un juge, après contestation, valide la demande d'accès du gouvernement américain à des données françaises, publiques ou privées, avez-vous l'obligation légale de les transmettre ?

Mme Corine de Bilbao. Un cadre légal limite grandement la possibilité de donner suite à la demande. Celle-ci est transmise au client ; pour ce qui nous concerne, encore faut-il que nous soyons techniquement capables d'y répondre… Microsoft est dans l'impossibilité de fournir les données lorsque des clés de chiffrement ont été utilisées et que celles-ci sont dans le coffre du client, dans le cadre du *confidential computing*, ou lorsqu'elles sont hébergées dans un *cloud* sécurisé, certifié SecNumCloud. Entre les conditions juridiques, les engagements contractuels, par lesquels nous contestons les demandes devant les tribunaux – nous avons obtenu gain de cause devant la justice fédérale américaine au sujet d'une ordonnance relevant du Fisa – et les contraintes techniques, la possibilité que les données soient transmises est pratiquement réduite à néant. Ainsi, nous n'avons jamais communiqué de données émanant d'administrations publiques européennes. Je vous invite à consulter le rapport de transparence que nous vous transmettrons. Cela permettra de compléter mes propos.

Mme Cyrielle Chatelain, rapporteure. Le sujet est complexe, et j'ai indiqué qu'un autre volet de mes questions porterait sur les aspects techniques. Ma question renvoyait au cadre juridique : êtes-vous soumis à l'obligation légale de transmettre les données, qu'elles soient publiques ou privées, lorsque la demande a été validée par le juge ? Rappelons qu'un grand nombre de Français peuvent stocker leurs données dans les *clouds* de vos entreprises. J'aimerais donc que vous répondiez précisément à cette question sur votre responsabilité légale.

M. le président Philippe Latombe. Autrement dit, transmettez-vous les données, qu'elles soient chiffrées ou non, à l'autorité judiciaire américaine ou à l'agence fédérale qui vous en a fait la demande, une fois que toutes les voies de recours ont été épuisées ?

Mme Corine de Bilbao. Je vais sans doute me répéter, mais nous contestons ces demandes devant les tribunaux. S'agissant des administrations publiques, nous n'avons pas de cas où les données ont été transmises. Pour les entreprises privées, nous avons un cas dans les trois dernières années.

Mme Cyrielle Chatelain, rapporteure. Vous avez donc une obligation légale de transmission…

Mme Corine de Bilbao. J'essaie de vous apporter une réponse concrète, mais je ne suis pas une spécialiste de cette question. Je propose de vous transmettre une réponse plus détaillée par écrit. En vertu de la *comity*, autrement dit du principe de courtoisie internationale, nous devons nous conformer aux obligations des différents États où nous opérons.

Mme Cyrielle Chatelain, rapporteure. Je vous remercie d'avoir pris la parole en premier. Cette question n'est pas la plus simple, et je vois bien que la réponse est difficile à donner. Vous nous dites devoir vous conformer aux obligations des États dans lesquels votre entreprise exerce ses activités, mais son siège se trouve aux États-Unis. Si vous avez épuisé les voies de recours, il vous reste deux options : soit obéir au juge et à la loi américaine, soit désobéir. Quel serait votre choix ?

M. Arnaud David. Cette question ne s'est pas posée à nous, puisque, comme je l'ai indiqué au sujet de nos rapports de transparence, nous n'avons pas fourni de données de clients, qu'il s'agisse d'entreprises ou de gouvernements, situés en dehors des États-Unis, en réponse à des demandes du gouvernement américain.

Cela reste donc une hypothèse. J'entends que vous distinguiez cadre légal et cadre technique mais, comme vous le savez, dans tout cadre légal, il y a des exceptions. En l'occurrence, selon la loi, on ne peut fournir des données que dans la mesure où on y a accès sur le plan technique. Tout est lié.

Pour ce qui nous concerne, des solutions sont appliquées systématiquement, dont certaines sont intégrées dans nos serveurs comme AWS Nitro, qui nous empêchent d'accéder aux données de nos clients. Dans le cas que vous évoquez, nous serions dans l'impossibilité technique de répondre aux demandes formulées. Par ailleurs, il existe des solutions de chiffrement, que les clés soient managées par les services d'AWS ou stockées auprès de prestataires comme Devoteam ou Thales.

Nos actions consistent à faire en sorte que les demandes soient redirigées vers le client. Nous considérons en effet que nous n'avons pas de légitimité pour y répondre, dans la mesure où nous n'avons pas accès aux données. Les clients sont plus à même de le faire – prenons le cas d'un opérateur de forums ou de réseaux sociaux, qui a une relation directe avec ses utilisateurs finaux.

M. Frédéric Geraud de Lescazes. Google Cloud respecte l'État de droit : si un juge allemand, canadien, chilien, américain ou français nous demande de coopérer, nous le faisons. Nous nous conformons au droit. En France, sur une année courante, nous recevons près de 15 000 demandes – demandes d'informations, réquisitions judiciaires et administratives. Nous répondons à 80 % d'entre elles, avec diligence. Si 20 % restent sans réponse, c'est parce que le contenu a disparu, que le compte a été fermé ou que la demande a été mal libellée. Nous collaborons avec chacune des juridictions nationales des pays où nous avons décidé d'opérer en tant qu'acteur économique. Nous répondons aux demandes des juges, même si le matériel est inexploitable.

M. le président Philippe Latombe. Là encore, je note une hétérogénéité dans vos réponses. Je ne vois pas comment vous pouvez faire figurer dans un rapport un décompte à l'unité près sachant que certaines demandes relevant du Cloud Act ou du Fisa sont formulées dans un cadre secret. Tout cela signifierait que le Cloud Act et le Fisa ne servent à rien ! Je suis très rassuré et heureux de vous l'entendre dire sous serment… Mais si c'est bien le cas, on ne voit pas trop pourquoi le Cloud Act a été intégré, en tant que cavalier législatif, dans un texte budgétaire pendant le mandat d'un président à nouveau en exercice. On ne comprend pas non plus pourquoi le Congrès prend la peine de rediscuter en ce moment même du Fisa.

Mme Cyrielle Chatelain, rapporteure. Nous n'avons pas la même lecture, monsieur le président. Je constate qu'une seule entreprise a reconnu qu'elle coopérerait avec la justice, alors que c'est le cas de toute entreprise, me semble-t-il… Je remercie son représentant de l'avoir assumé. Pour les autres, le fait qu'à trois reprises, à une question très précise qui appelait simplement un « oui » ou un « non », il n'y ait pas eu de réponse est une réponse : oui, vous accepteriez de transmettre des données à la justice.

Vos entreprises se livrent à des activités de lobbying, de manière intensive et en toute transparence, notamment auprès de l'Union européenne. Adhérez-vous à la position de la Computer and Communications Industry Association (CCIA), dont vous êtes membres ? Dans un communiqué de presse de décembre 2025, elle appelait à opérer sans attendre une simplification digitale, laquelle vise, de notre point de vue, un affaiblissement ou une révision à la baisse des exigences du RGPD et l'AI Act. Les rendez-vous que vous prenez sont connus, mais nous aimerions savoir dans quel sens vous plaidez une fois la porte refermée.

M. Frédéric Geraud de Lescazes. Google est membre de la CCIA, organisation professionnelle qu'on qualifierait plutôt de « corps intermédiaire » en français. Ce syndicat comporte des groupes de travail thématiques, qui se réunissent pour établir une position commune concernant des projets de lois ou de réglementations. Chaque membre apporte sa contribution et, comme dans toute organisation professionnelle, c'est le plus souvent ceux qui s'engagent et qui travaillent le plus qui tiennent la plume. La position d'un syndicat professionnel reflète généralement celle de ses principaux membres. Pour dire les choses très simplement, la position de la CCIA reflète une partie des positions de Google.

Mme Corine de Bilbao. Nous considérons que le RGPD est une bonne réglementation ; nous avons d'ailleurs été l'une des premières entreprises à l'adopter, et nous l'avons même appliqué au niveau mondial. Nous nous conformons aux réglementations – nous ne pourrions pas opérer depuis quarante ans dans certains pays européens comme l'Allemagne, le Royaume-Uni ou la France sans nous y conformer. S'agissant de l'AI Act, nous attendons que sa mise en place soit achevée.

Nous avons démontré depuis de nombreuses années notre capacité à nous adapter aux réglementations. Ce qui nous importe, c'est qu'elles n'entrent pas en contradiction avec d'autres législations et que, du point de vue du business, elles soient lisibles et facilement applicables chez nos clients.

M. Arnaud David. Je ferai une réponse similaire. Il n'est pas question pour nous de soutenir une quelconque dérégulation. Nos positions reflètent aussi ce que nous disent les entreprises et nos clients en général. Il convient de faire en sorte que la conformité avec les réglementations repose sur des processus harmonisés en Europe. Je prendrai un exemple à propos d'un aspect qui fait actuellement l'objet de discussions dans le cadre de l'omnibus numérique : nous aimerions que le rapport d'évaluation des risques établi au titre du RGPD puisse servir de base au rapport d'évaluation directe demandé dans le cadre de l'AI Act. Il s'agit simplement d'éviter d'avoir à faire deux fois le même travail. Ce sont donc plutôt des considérations de bon sens qui nous guident ; cela ne va pas plus loin que ça.

M. le président Philippe Latombe. Me voilà rassuré !

Mme Cyrielle Chatelain, rapporteure. Vous respectez la loi, ce qui est normal. J'imagine que les sommes dépensées pour le lobbying ont aussi vocation à appeler l'attention sur les contraintes qu'implique le RGPD pour les entreprises du numérique.

Je suis ravie de vous entendre dire, madame de Bilbao, que le RGPD fonctionne bien. S'il ne s'agit que d'éviter des doublons dans les rapports, je vous garantis qu'il n'y aura pas de difficultés particulières. Ce qui nous inquiète davantage, c'est la modification de la définition des données personnelles. Lors de notre déplacement à Bruxelles, il y a quelques semaines, il nous a été indiqué que les propositions écrites, sans études préalables ni analyses extérieures, reprenaient plutôt les demandes conjointes des grands opérateurs que vous êtes, relayées

notamment par vos syndicats ou vos corps intermédiaires. Si vous vous retrouvez globalement dans les positions défendues par la CCIA, on peut penser que vos souhaits vont au-delà d'une simplification de la rédaction des rapports.

J'aimerais vous interroger sur votre modèle économique. Dans un avis portant sur le fonctionnement concurrentiel de l'informatique en nuage, l'Autorité de la concurrence a relevé plusieurs problèmes : manque de transparence sur les tarifs ; crédits *cloud* très importants accordés aux start-up ; systèmes de licence rendant plus coûteuse l'utilisation de produits dans des environnements cloud concurrents, notamment pour Microsoft ; pour Amazon, mises à jour unilatérales de certains services faisant office de standard technique, auxquelles les autres acteurs ont accès avec un délai. Depuis la publication de cet avis, en 2023, vos pratiques ont-elles évolué ?

Google Cloud a déposé une plainte contre Microsoft auprès de la Commission européenne. Celle-ci a ensuite été retirée, non parce que les griefs n'étaient plus fondés, mais parce que la Commission européenne elle-même a voulu se saisir du sujet. Pourriez-vous nous expliquer les raisons pour lesquelles Google Cloud avait déposé plainte ? Où en sont les travaux de la Commission européenne sur ce sujet ?

Lors d'une audition précédente, le DSI d'une grande organisation nous a expliqué qu'il avait constaté une augmentation tarifaire de 20 % entre le nouveau et l'ancien contrat passé avec Microsoft, à périmètre identique. Il nous a précisé que Microsoft demandait expressément qu'il ne soit pas fait état de ces augmentations ; étant sous serment, il a été contraint de nous transmettre cette information, par souci de transparence. Pourquoi demander aux acteurs, notamment aux acteurs publics, de ne pas communiquer à ce sujet ? Qu'est-ce qui peut justifier une telle augmentation ?

Mme Corine de Bilbao. Pour ce qui est de la transparence des prix, nos prix de licences et de services *cloud* sont publiés sur un site que je pourrai vous indiquer. Ils sont calculés en dollars, puis convertis en euros pour l'Europe. Ce même site indique les remises consenties en fonction du volume. La transparence des prix est donc complète et accessible à tous nos clients, privés comme publics.

Quant aux augmentations de prix, elles existent, comme dans toute industrie, et sont liées à trois facteurs. Le premier est l'enrichissement des logiciels, des produits et des services, et pas seulement sur le plan de la sécurité. Le deuxième est lié, comme dans toute industrie, à l'augmentation des coûts de matériel, de personnel et d'investissement. Le troisième est l'évolution des taux de change. Nous sommes transparents sur les augmentations de prix. La dernière, qui a eu lieu en 2023, était de 11 %, en raison du taux de change entre l'euro et le dollar. Je précise qu'une fois les contrats signés, que ce soit pour trois ou cinq ans, les prix sont évidemment connus sur leur durée de validité – c'est ce que nous demandent nos clients. On a moins dit que de nouveaux taux de change ont entraîné, si ma mémoire est bonne, une baisse de prix de l'ordre de 7,6 % en février 2026. Je répète toutefois que nos prix sont finalisés dans des contrats et valables pour la durée de ceux-ci, que nos clients soient publics ou privés, étant précisé que, pour les clients publics, cela passe par des distributeurs et des partenaires.

J'en viens à votre troisième question, qui portait sur l'Autorité de la concurrence. Des discussions ont eu lieu en 2024, et un accord a été trouvé avec plusieurs fournisseurs de *cloud*, dont OVH et l'association CISPE, à propos de Windows Server. Je n'en ai pas les détails mais, cet accord ayant été trouvé, le sujet est clos. Il faudrait poser la question à Google, qui avait déposé une plainte avant de la retirer. Nous estimons, pour notre part, qu'il n'y avait pas de base juridique, mais je propose de laisser les représentants de Google répondre sur ce point spécifique.

Mme Cyrielle Chatelain, rapporteure. La mise à jour Windows 11 a donné lieu à tout un débat, parce qu'elle ne pouvait pas être installée sur certains matériels un peu anciens mais fonctionnels. Cette question se posera à nouveau. Windows 10 deviendra-t-il payant pour les personnes qui ne pourraient pas basculer vers Windows 11 ?

Mme Corine de Bilbao. Sur cette question technique, je laisse M. Philippe Limantour répondre.

M. Philippe Limantour, directeur technologie et cybersécurité de Microsoft France. La sécurité est notre principal souci. L'Anssi a déclaré qu'une « racine de confiance matérielle » de Windows 10 était vulnérable à des attaques, ce qui signifie que toute personne ayant accès à une machine équipée de cette ancienne technologie peut accéder aux données, quel que soit d'ailleurs le système d'exploitation – Linux, Windows ou autre – utilisé sur ce matériel. Nos systèmes d'exploitation ayant une durée de vie d'à peu près dix ans, souvent rallongée – celle de Windows 10 l'a été de trois ans –, nous ne pouvions pas nous permettre, au passage à Windows 11, d'aller contre l'avis de l'Anssi et d'autres autorités de sécurité. Une nouvelle puce, dénommée TPM 2.0, était nécessaire pour assurer la sécurité des données de nos clients.

Mme Cyrielle Chatelain, rapporteure. Alors, Windows 10 sera-t-il payant ?

M. Philippe Limantour. Des extensions de support pour la sécurité ont été proposées aux entreprises et aux particuliers qui restent en Windows 10, avec des extensions gratuites pour ces derniers. Les entreprises peuvent continuer d'utiliser ces matériels dans d'autres conditions si elles acceptent les risques de sécurité y afférents.

M. le président Philippe Latombe. Je suis heureux de noter que l'augmentation de tarifs de 2025 paie une partie de CrowdStrike.

M. Julien Lépine. Vous nous avez d'abord interrogés sur le manque de clarté des tarifs. Depuis la création d'AWS, notre catalogue de prix est complètement public et disponible en ligne pour l'ensemble de nos clients. C'est vraiment l'un des fondamentaux, en quelque sorte l'ADN d'Amazon, que le prix soit affiché publiquement et disponible sur un site internet. Comme chez tout commerçant, les prix baissent en fonction du volume acheté. Il y a eu 161 baisses de prix depuis la création de la plateforme : notre logique est donc plutôt de faire profiter nos clients, par des baisses de prix, des bénéfices que nous réalisons grâce à l'effet d'échelle.

Pour certains contrôleurs de gestion, un catalogue de prix où chaque service a un prix différent, certains étant facturés à la milliseconde, peut représenter une certaine complexité. Nous fournissons donc aussi un ensemble d'outils permettant de planifier, de décrire une architecture technique et d'obtenir une estimation du prix. Le but est que le client puisse faire un choix éclairé, sans engagement. Une fois que le client a commencé à travailler, il dispose d'outils de suivi qui lui donnent une vision du budget consommé et lui permettent de savoir si les dépenses dépassent le budget estimé. Nous avons donc vraiment travaillé sur ces points pour aider les clients, et sommes vraiment des avocats de la plus grande transparence possible sur le coût de nos services – je préfère ce mot à celui de « tarifs », auquel la géopolitique donne actuellement une signification un peu différente.

Vous évoquiez, en deuxième lieu, les crédits, qui ont effectivement donné lieu à un certain nombre d'analyses du point de vue de la concurrence. Les crédits sont un moyen, en

particulier pour les PME, de venir essayer une plateforme, sans engagement. Dans les incubateurs, les start-up peuvent tester des crédits différents sur plusieurs plateformes, et plus de 80 % des entreprises recourent déjà au *multicloud*.

Une question qui nous était spécifiquement destinée portait sur les mises à jour unilatérales. Je ne connais pas en détail le cas précis qui a été évoqué, mais nous avons un certain nombre de réponses à vous apporter.

Si vous avez commencé à utiliser Amazon S3 – notre service de stockage Simple Storage Service, premier service sorti par AWS en mars 2006 – il y a vingt ans, vous pouvez continuer à l'utiliser de la même manière en 2026, avec exactement les mêmes appels, la seule différence concernant le niveau de sécurité. En 2006, en effet, les standards de sécurité du chiffrement n'étaient pas encore post-quantiques, car la question ne se posait pas. Ainsi, nous avons procédé à des mises à jour pour le chiffrement, mais le fondamental de l'API (interface de programmation d'application) reste le même.

Deuxième point important pour nous : les SDK, ou *software development kits,* qui permettent d'intégrer la plateforme AWS à une application ou à un développement logiciel, sont *open source* depuis leur création, auditables et téléchargeables. Nous avons travaillé avec des plateformes comme Terraform pour laisser le libre choix aux clients.

Je laisse Arnaud David vous parler des licences.

M. Arnaud David. Les pratiques déloyales en matière de licences de logiciels sont un problème pour nos clients, rapporté depuis déjà de nombreuses années, mais ce problème n'est pas lié au *cloud*. En soi, une licence de logiciel, c'est du code ; elle devrait donc être portable quel que soit l'environnement – sur site, dans le *cloud* ou ailleurs. Il faut également distinguer ces licences des environnements *cloud*, constitués d'une somme non seulement de logiciels, mais aussi de matériels, de réseaux et de dispositifs de sécurité qui s'exécutent dans un environnement spécifique. Mélanger ces deux réalités assez distinctes brouille le contexte et évite de mettre en lumière le problème des restrictions liées aux licences logicielles. Cela a été constaté par plusieurs organisations : outre l'Autorité de la concurrence, que vous avez citée, son homologue anglaise s'en est elle aussi saisie récemment, et le Cigref l'avait fait voilà quelques années également. Il s'agit donc d'un problème important, sur lequel il conviendrait effectivement d'agir.

Mme Cyrielle Chatelain, rapporteure. Les *egress fees,* autrement dit les frais pour des données sortantes, sont-ils toujours appliqués ? Si oui, à combien s'élèvent-ils ?

M. Arnaud David. Le principe est qu'AWS n'est pas au courant de l'utilisation que les clients font de ses services. Lorsqu'un client reprend ses données – ce qu'on appelle un « *data transfer out* » –, il peut le faire pour de nombreuses raisons, notamment parce qu'il souhaite quitter les services d'AWS, mais pas uniquement. Depuis l'origine, nous facturons cette utilisation de nos services ; en revanche, AWS ne facturait pas de frais de résiliation lorsque le client souhaitait quitter ses services. Nous avions donc instauré, de manière générale et hors cas de résiliation, des réductions en garantissant 100 gigaoctets par mois sans frais. Cette mesure s'appliquait depuis quelques années, et je crois qu'elle est d'ailleurs toujours applicable.

D'autres éléments sont venus s'y ajouter dans le cadre des discussions, notamment, de la réglementation Data Free Flow with Trust, puis du Data Act. Quelle que soit la raison de facturer l'utilisation d'un service, nous avons anticipé la réglementation entrée en vigueur en

septembre 2025 et celle qui s'appliquera dans trois ans pour les frais de transfert, même s'il ne s'agissait pas de frais de résiliation, en permettant aux clients de quitter sans frais les services AWS s'ils le souhaitent et de recourir à leur gré à plusieurs solutions *cloud* en même temps – c'est ce qu'on appelle le *multicloud* –, au prix et en conformité avec la réglementation du Data Act.

Pour répondre à votre question, il n'y a donc pas de frais de sortie facturés.

M. Frédéric Geraud de Lescazes. Comme ceux de nos concurrents, nos prix sont publics et en ligne. Il y a un peu plus d'un an, l'Insee s'est rapproché de nous pour élaborer un indice de prix ; depuis lors, nous participons trimestriellement à la production de cette cohorte statistique en cours de mise en place. Comme vous pourrez le vérifier auprès de l'Insee, nos prix ne bougent pas depuis plusieurs trimestres. Du reste, lors de la crise énergétique, en 2022, nous n'avons pas augmenté nos prix, contrairement à certains de nos concurrents.

Comme vous l'a dit Sébastien Missoffe, c'est notre position de marché – de l'ordre de 10 % de parts de marché – qui guide notre stratégie. Nous avons donc fait clair et simple pour la partie relevant du Data Act, parce que nous voulons faire bouger le marché. Ainsi, nous avons été les premiers, par anticipation, à mettre fin aux coûts de sortie : lorsque le contrat avec le fournisseur *cloud* se termine et que le client doit migrer ses données en dehors pour qu'elles reviennent chez lui ou aillent chez un autre fournisseur, les frais ont été réduits à zéro. Nous avons beaucoup communiqué à l'époque et avons fait bouger les autres acteurs du secteur, qui ont été, dans les mois qui ont suivi, obligés de nous imiter.

Nous avons fait la même chose pour les *egress fees* facturés en cas de *multicloud*. Là encore, compte tenu de notre position de marché, nous sommes en faveur du *multicloud*. De fait, au-delà de l'aspect sécuritaire – il est conseillé de ne pas mettre tous ses œufs dans le même panier pour éviter de créer un seul point de rupture, un « *single point of failure* », sur le plan de la cybersécurité –, il est de notre intérêt d'offrir nos technologies. Nous avons donc réduit les frais à zéro. Là encore, nous étions les premiers à le faire, et nous avons emmené le marché. Nous essayons d'être différents pour attirer de nouveaux clients. C'est notre intérêt.

S'agissant des crédits *cloud*, je vous renvoie à une disposition de la loi Sren. Au cours des débats parlementaires, la Commission européenne a écrit par deux fois à la France pour lui expliquer que les dispositions qu'elle s'apprêtait à prendre en la matière étaient une surtransposition, puisque ces crédits n'étaient pas prévus dans le texte du Data Act, et qu'elles ne pourraient donc s'appliquer qu'aux acteurs facturant depuis la France. À cet égard aussi, donc, nous sommes différents : Google Cloud France SARL facture depuis la rue de Clichy, sous législation française, alors qu'à ma connaissance, AWS facture depuis le Luxembourg et Microsoft depuis l'Irlande. En somme, Google Cloud est donc le seul *hyperscaler* concerné.

En matière de coûts de sortie, nous sommes aussi signataires du code Swipo (Switching Cloud Providers and Porting Data), qui a été travaillé au niveau européen.

Quant à la plainte que nous avons retirée sur indication de la direction générale (DG) Concurrence de la Commission européenne, c'est pour nous une question de principe. Quel que soit l'acteur en cause, nous contestons la barrière que nous rencontrons et que rencontrent tous les acteurs sur ce marché.

M. le président Philippe Latombe. Est-ce à dire que si la DG Concurrence ne va pas au-delà de ce qu'elle fait actuellement, et que s'il n'y a pas de sanction ou de modification législative, vous pourriez reprendre votre plainte ?

M. Frédéric Geraud de Lescazes. La DG Concurrence nous a invités à retirer notre plainte, en nous indiquant que d'autres textes pourraient être le lieu approprié pour régler la question des licences juridiques déloyales.

M. le président Philippe Latombe. Mais si comme sœur Anne vous ne voyiez rien venir, reprendriez-vous votre plainte ?

M. Frédéric Geraud de Lescazes. Je ne sais pas répondre à votre question. Notre position est que ce combat est trop important pour que nous ne le continuions pas. J'aurais tendance à vous répondre que oui, à ce moment-là, nous remonterions au créneau… Mais nous espérons que certains textes aboutiront d'ici là pour régler la situation.

M. Aurélien Taché (LFI-NFP). Comme cela a été dit, l'État français et les Français hébergent une part croissante de leurs données sur vos infrastructures. Compte tenu des réponses que vous avez faites aux questions du président et de la rapporteure, je comprends qu'en cas d'injonction américaine de transmettre, au titre du Cloud Act ou du Fisa, les données des Français hébergées sur vos infrastructures, après la décision d'un juge, vous obtempéreriez. Vous n'avez pas répondu en disant que vous pourriez, dans ce cas, offrir aux Français une garantie juridiquement opposable – si je dis quelque chose de faux, merci de me contredire.

J'irai un peu plus loin dans la question. La plupart de vos entreprises ont financé la campagne de l'actuel président des États-Unis d'Amérique. Que se passerait-il en cas de conflit politique ou diplomatique majeur entre la France et ce pays ? Pouvez-vous garantir une continuité du service de vos entreprises dans ce cas précis ? La question paraît un peu surréaliste, mais je suis obligé de l'évoquer quand le président des États-Unis dit qu'il faut rebaptiser le golfe du Mexique en « golfe d'Amérique », puisque nous avons dans les Caraïbes des empreintes françaises, notamment les Antilles. Un conflit direct ou un conflit diplomatique majeur peut arriver – on le voit avec le juge Guillou qui, pour avoir fait appliquer le droit international, s'est vu couper ses moyens de paiement en application des lois extraterritoriales américaines. Comment réagiriez-vous à une injonction de l'administration américaine d'activer le *kill switch* et de ne plus assurer la continuité du service ? Quelles garanties pouvez-vous nous donner face à une telle hypothèse ? Quels sont les scénarios que vous avez documentés ? Étant des entreprises sérieuses disposant de moyens importants, vous avez certainement réfléchi à cette hypothèse…

M. Arnaud David. Pour ce qui est du contexte, nous fournissons des services aux organisations et aux entreprises, et avons donc été interrogés par nos clients à ce propos. Cette question est bien évidemment importante, mais elle occulte une réalité évoquée à plusieurs reprises : l'interdépendance, à de multiples niveaux, entre les États-Unis et l'Europe. AWS est une entreprise globale, qui a trente-neuf régions *cloud* dans le monde. Nous dépendons d'une chaîne de fournisseurs très variés dans de très nombreux pays, et nous investissons massivement dans des centres de données dans les pays où nous sommes présents, en France comme en Europe. Ce sont des investissements à long terme, qui nous engagent pour des durées de dix à quinze ans, voire plus. Le point fondamental est que nos clients comptent sur nous, comme vous le rappeliez, pour continuer à fournir les services en toutes circonstances.

Dans les cas où cette continuité de service serait menacée – de tels cas ne se sont, pour ce qui nous concerne, jamais réalisés –, nous prenons l'engagement ferme de mettre, en pratique, tout en œuvre pour continuer à fournir le service. Cet engagement, qui prendra probablement différentes formes en fonction de la situation, est très important.

Pour les clients qui souhaiteraient des garanties supplémentaires, nous avons lancé tout récemment, en janvier, comme nous l'avons rappelé dans nos propos liminaires, le *cloud* souverain européen, infrastructure dont les premiers centres de données sont basés en Allemagne – mais nous en avons annoncé d'autres dans d'autres pays européens – et qui se veut être un nouveau *cloud* pour l'Europe. Dans ce cadre, les infrastructures, le personnel et le management sont en Europe.

Cette infrastructure bénéficie aussi d'un réplicat du code source, ce qui signifie qu'elle n'a pas de dépendance critique vis-à-vis de nos autres infrastructures, en particulier aux États-Unis. Dans le cas d'une déconnexion mondiale de l'Europe, il y aurait tout ce qui est nécessaire pour continuer à opérer le service en Europe – c'est là un point fondamental.

J'ajouterai deux éléments supplémentaires. Du point de vue contractuel, pour les clients de ce nouveau *cloud* pour l'Europe, nous prenons l'engagement ferme que, si nous devions mettre fin à tout ou partie des services fournis par celui-ci, nous ne pourrions le faire qu'avec un préavis de douze mois, ce qui laisse de la visibilité aux entreprises.

Enfin, un détail qui ne remet pas en cause la question que vous venez de poser, mais qui a son importance : une étude publiée en février par le ministère néerlandais de la justice a analysé ce nouveau *cloud* au regard d'événements qui pourraient conduire à une rupture de continuité, et a qualifié ces événements d'improbables. Je ne veux pas dire que cela n'arrivera jamais, mais je tenais à signaler cet élément à votre attention.

M. le président Philippe Latombe. Le juge Guillou peut-il bénéficier des services d'AWS ? Outre la livraison de colis par Amazon, a-t-il accès à votre suite et à du stockage ?

M. Arnaud David. Je ne peux pas répondre à votre question, parce que nos clients sont principalement des entreprises. Or je ne sais pas si le juge Guillou a une entreprise qui souhaiterait utiliser les services d'AWS…

M. le président Philippe Latombe. On va lui demander de créer une entreprise unipersonnelle à responsabilité limitée (EURL) en France, qui pourra peut-être utiliser les services d'AWS !

M. Frédéric Geraud de Lescazes. Le système américain de financement électoral est très différent du nôtre. Ce financement passe principalement par les employés de l'entreprise regroupés dans ce qu'on appelle, je crois, des *political action committees* (PAC). C'est un processus que je ne connais pas très bien. Puisque le système américain est bipartisan, il existe un groupe républicain et un groupe démocrate, et nos employés financent par ce biais les campagnes électorales tant au niveau des États qu'au niveau fédéral, comme dans toutes les entreprises présentes sur le sol américain. Ce n'est pas plutôt l'un ou plutôt l'autre, mais les deux. Typiquement, la Californie est majoritairement démocrate, mais ce n'est pas le cas d'autres États. Ces choses évoluent dans le temps. J'ai toujours entendu parler du système bipartisan, mais il existe d'autres partis politiques aux États-Unis ; au vu du nombre de nos employés, il existe peut-être aussi un PAC pour ceux-là.

Pour ce qui est du *kill switch*, je rappelle que, dans le discours par lequel il lançait, en 2021, la doctrine « Cloud au centre », Bruno Le Maire a pris l'exemple du nucléaire français, soulignant notamment que dans les années 1950, pendant le mandat du général de Gaulle, ou du moins à l'époque d'une « certaine idée de la France », EDF, qui avait développé sa propre technologie de nucléaire civil, avait fait le choix conscient d'acheter des licences américaines

de l'entreprise Westinghouse. Aujourd'hui, en 2026, l'ensemble du parc nucléaire civil français, hors EPR de nouvelle génération, tourne encore sur des licences Westinghouse. La question du *kill switch* est donc majeure et fondamentale : pourrons-nous allumer la lumière demain matin ?

Pour ce qui nous concerne – et c'est ce qui nous place peut-être dans une position plus confortable que nos concurrents –, notre solution « dans une bulle d'air », que j'ai déjà évoquée, est complètement déconnectée. Elle n'est donc pas déconnectable !

Je veux aussi citer les travaux liés au SecNumCloud. L'Anssi, qui travaille sérieusement, n'a pas attendu tel type de mouvement politique dans tel pays pour prévoir, dès le début de 2016, l'obligation d'un plan de réversibilité. La question de savoir comment continuer si l'on n'a plus accès à ces technologies fait partie intégrante du SecNumCloud. Outre notre offre préexistante, Google Cloud Platform, totalement déconnectée, vous pouvez donc aussi accéder à des technologies qualifiées SecNumCloud, localisées dans la filiale de Thales dénommée S3NS. En cas de *kill switch*, rien ne serait simple, et toute migration serait fort complexe, mais ces deux solutions existent.

Pour ce qui est des services de Google Cloud Platform en direct, nous avons pris l'engagement, en réponse aux craintes qui se sont exprimées – nous ne sommes pas aveugles aux tumultes du monde –, de fournir à nos clients, en cas d'interruption de nos services, l'accès à notre code pour qu'ils puissent, s'ils disposent des ingénieurs nécessaires, assurer la continuité du service. Ce ne sera pas simple, mais c'est notre engagement.

M. le président Philippe Latombe. Je vous poserai la même question qu'à AWS : avez-vous appliqué au juge Guillou la réglementation américaine, et lui avez-vous coupé l'accès à toute solution Google ?

M. Frédéric Geraud de Lescazes. En l'occurrence, il s'agit plutôt du compte mail. Nous offrons à tous nos utilisateurs, qu'ils soient ou non juges à la CPI, la possibilité de récupérer leurs données dans un format utilisable et interopérable pour qu'ils puissent migrer vers une autre solution, car nos technologies sont basées sur de l'*open source*. Si la loi le permet, nous prévenons l'utilisateur et lui fournissons le pas-à-pas pour migrer ses données. Si nous disposons des précisions suffisantes – par exemple, dans le cas d'une décision judiciaire –, nous lui indiquons à quelle date il doit effectuer telle action. Si la loi ne le permet pas, nous respectons l'État de droit, et nous appliquons la loi.

M. le président Philippe Latombe. Ce qui veut dire, en l'état actuel des choses, que le juge Guillou ne pourrait pas ouvrir un compte Gmail ni utiliser la suite de Google s'il le demandait, même à titre particulier.

M. Frédéric Geraud de Lescazes. Tout à fait.

Mme Corine de Bilbao. La probabilité d'un *kill switch* est extrêmement faible, voire inexistante. Microsoft est une entreprise globale, qui opère dans 180 pays et s'est engagée à augmenter de 40 % ses centres de données en Europe d'ici à 2027. Au vu du montant de nos investissements, il serait suicidaire d'appliquer un *kill switch*. L'entreprise n'est pas le gouvernement américain.

Cela dit, cette préoccupation arrive chez nos clients, et nous devons répondre à leurs questions. Nous le faisons de plusieurs manières. D'abord, sur le plan contractuel, nous avons pris des engagements de résilience envers nos clients du secteur public, mais aussi des services et infrastructures critiques au niveau européen. Nous avons également un conseil d'administration avec des Européens pour les *data centers*. À cela s'ajoutent des engagements techniques, avec une panoplie de possibilités en fonction de la localisation des clients. Je propose que Philippe Limantour vous décrive ces engagements techniques qui permettent aux clients de se protéger d'un *kill switch*.

M. le président Philippe Latombe. Cela signifie donc qu'il n'y a pas eu de *kill switch* de la part de Microsoft pour une entreprise indienne, une université chinoise, la CPI et, éventuellement, certains de ses juges, parce que le *kill switch* n'existe pas ?

Mme Corine de Bilbao. Pour ce qui concerne notamment l'entreprise indienne, je n'ai pas d'informations, car ce n'est pas dans ma zone de travail, mais nous vous en communiquerons. En revanche, pour ce qui concerne la CPI, Microsoft n'a pas coupé les services. C'est tout ce que je peux vous dire. Si vous avez besoin de plus d'informations sur cette question, qui ne relève pas de mon champ de compétence, nous vous ferons parvenir une note.

M. Philippe Limantour. Concernant la résilience, il existe effectivement pour nos clients plusieurs moyens de se prémunir d'un *kill switch* et d'assurer la continuité de l'activité.

Il est tout d'abord possible d'utiliser des mécaniques complètement déconnectées, que nous proposons nous aussi. Vous pouvez en effet installer dans vos propres centres de données une solution, Azure Local, qui permet d'être entièrement déconnecté de la plateforme Microsoft. Le matériel correspondant à cette solution est acheté auprès de revendeurs ; le client, public ou privé, en est donc entièrement propriétaire. Il peut également faire tourner sur ce matériel des logiciels de collaboration ou de partage SharePoint – c'est la solution Microsoft 365 local.

Il existe aussi des licences dites *on-premise* (sur site), où les données ne sont pas dans le *cloud*.

Le troisième moyen de se prémunir d'un *kill switch* passe également par SecNumCloud : l'entreprise Bleu a des plans de résilience et est complètement autonome pour servir ses clients, leur apporter un support et les facturer pour continuer les activités sur base de technologie Microsoft. Il y a une séparation complète entre l'opérateur et le fournisseur de technologie : nous fournissons la technologie à Bleu, qui est complètement autonome de Microsoft pour l'opérer.

M. le président Philippe Latombe. Quand Bleu sera arrivé à l'Assemblée…

M. Philippe Limantour. Pardon, mais Bleu est déjà là. Il faudrait dire : « quand Bleu aura la qualification SecNumCloud ».

M. le président Philippe Latombe. Vous avez un peu anticipé…

Madame de Bilbao, avec les réponses que vous nous donnerez à propos de l'entreprise indienne, pourriez-vous aussi nous dire quels sont les services auxquels le juge Guillou pourrait avoir accès ? Nous lui transmettrons ces éléments, ce qui lui permettra éventuellement de

trouver des solutions. Je ne dis pas cela méchamment, mais si vous avez des solutions, nous sommes preneurs…

M. Nicolas Bonnet (EcoS). Après cette promenade dans les nuages à travers le *cloud*, je vais essayer de nous ramener un peu sur terre car, derrière la dématérialisation, il y a bien du matériel informatique. Vous n'êtes pas sans savoir – et vous l'avez d'ailleurs évoqué – que les appels de puissance et de stockage sont de plus en plus importants. Vous souhaitez développer les *data centers* en Europe, et sans doute aussi ailleurs. Tout cela a un impact environnemental grandissant, puisque cela représente déjà 4,4 % de l'empreinte carbone de la France, du moins pour le numérique ; selon les prévisions de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) ou de l'Agence de la transition écologique (Ademe), le tendanciel, à l'horizon 2030, serait un triplement de l'empreinte carbone et un doublement de l'empreinte énergétique, alors qu'il faudrait au contraire diminuer fortement l'empreinte carbone pour respecter nos engagements climatiques.

Quelles actions entreprenez-vous pour que le numérique et l'IA, qui consomme une grande partie de la puissance de stockage et de calcul dans ce domaine, soient plus sobres en énergie et en ressources ? Avez-vous envisagé de vous appliquer la démarche qu'a engagée récemment Mistral, en travaillant avec l'Ademe sur une analyse du cycle de vie pour essayer d'objectiver davantage les efforts que chacun fait – ou ne fait pas – pour diminuer son empreinte carbone et sa consommation d'énergie ?

Si j'ai bien compris, vous représentez plutôt la partie *cloud* de vos entreprises : vous n'êtes donc *a priori* pas censés savoir ce que font vos clients. Pourriez-vous tout de même nous dire, du point de vue macro, quelle part des services que vous hébergez représentent respectivement, par exemple, les usages de services mail, d'IA générative accessible au grand public et d'IA appliquée à la recherche ? Quelqu'un a évoqué tout à l'heure la recherche sur le cancer, que nous considérons tous comme éminemment importante, mais je ne suis pas certain que, par rapport à la consommation de ressources et d'énergie de l'IA générative, de l'IA au sens large ou du *streaming* vidéo, sa part soit la plus grande. Pouvez-vous donc nous dire comment sont utilisées les puissances de calcul et de stockage dont vous disposez ?

Mme Cyrielle Chatelain, rapporteure. De combien de *data centers* êtes-vous les usagers uniques, que vous les possédiez déjà ou que vous en prévoyiez le développement ? Lorsque vous êtes en colocation, quel est votre pourcentage d'utilisation ?

Par ailleurs, s'agissant des projets que vous envisagez de développer en France, en propre ou en tant qu'actionnaires, quelle est la puissance énergétique de raccordement actuelle et quelle est la puissance demandée ?

M. Frédéric Geraud de Lescazes. Mistral n'a pas été le premier acteur du secteur à effectuer une analyse du cycle de vie, qui a été mondialement saluée. Quelques mois avant, Google avait analysé, étape par étape, la consommation énergétique de son modèle Gemini. La méthodologie utilisée a été rendue publique, en *open source*, afin de contribuer aux travaux mondiaux sur ces questions.

Google entretient une relation particulière avec la science : nous sommes nés d'un article de recherche publié en 1998, qui avait pour but de classer l'information disponible sur le web pour la rendre plus disponible, sans considération mercantile. Notre moteur de recherche est issu de la R&D. Au cours de deux dernières années, trois de nos collègues ont reçu un prix Nobel. Le plus récent est français : Michel Devoret a reçu le prix Nobel de physique pour ses

travaux sur le quantique. Notre éminent collègue dirige actuellement le département d'intelligence artificielle quantique de l'université de Californie, à Santa Barbara. Ses travaux de recherche fondamentale, menés dans les années 1980, ont été mis en production et ont débouché sur la fabrication d'une puce dénommée Willow – l'une des premières puces quantiques. Je le disais, la science est importante pour Google.

Notre forge à modèles d'intelligence artificielle, Google DeepMind, est installée à Londres. Son directeur général a reçu l'année dernière, avec un autre collègue et un chercheur d'un laboratoire britannique, le prix Nobel de chimie pour le développement d'une base de données nommée AlphaFold, qui a permis à des chercheurs germano-turcs de trouver un vaccin contre le covid. Cette base de données permet de prédire la forme d'une protéine parmi un total de 200 millions de formes. Plus de 65 000 scientifiques français y ont gratuitement accès chaque jour. Notre moteur, c'est de faire avancer la science. C'est aussi ce qui a prévalu dans notre décision de partager notre méthodologie d'analyse de la consommation énergétique liée aux usages de l'IA.

Sur le territoire français, Google Cloud n'est propriétaire d'aucune infrastructure ni d'aucun *data center*. Notre région Cloud Paris correspond à trois lieux de colocation chez des hébergeurs classiques, que je ne citerai pas.

Nous avons cependant des projets de développement d'infrastructures en France. Celui situé à Ozans, dans la communauté d'agglomération de Châteauroux Métropole, est public. Nous avons signé la promesse de vente et terminé les études techniques relatives au terrain, qui est majoritairement karstique. La majorité des études environnementales sont également finalisées. Nous avons découvert la présence d'une population de crapauds persillés, des batraciens plutôt rares ; un bureau d'études réfléchit déjà à la meilleure manière de traiter cette question.

Le comité de pilotage de ce projet de centre de données de Google a tenu sa première réunion le 5 février dernier, en présence de l'ensemble des élus locaux – du département et de la région – et de représentants de l'État. Il est coprésidé par le préfet de l'Indre, qui vient de changer, et le président de Châteauroux Métropole, Gil Avérous. Des infrastructures électriques devant être développées dans le cadre de ce projet, des représentants d'Enedis et de RTE y participent également. Nous avons choisi de mobiliser la Commission nationale du débat public (CNDP) ; trois garants ont été nommés, et les premières réunions auront probablement lieu à la rentrée prochaine.

Nous avons présenté au comité de pilotage l'intégralité de ce qui n'est qu'un projet – nous ne sommes pas pleinement propriétaires du terrain et n'avons pas encore obtenu de permis de construire. Le préfet a demandé à avoir la haute main sur ce projet industriel ; de manière générale, les services de l'État apportent un soutien appuyé.

Je propose de demander aux deux coprésidents du comité de pilotage de vous inviter à sa prochaine réunion, afin que vous ayez connaissance de toutes ces informations.

Mme Cyrielle Chatelain, rapporteure. La puissance énergétique est un enjeu essentiel, voire stratégique, pour le développement des *data centers*. De quelle puissance énergétique aurez-vous besoin pour alimenter cet immense projet – de 190 hectares, je crois ?

M. Frédéric Geraud de Lescazes. La surface est précisément de 195 hectares.

Nous nous sommes engagés auprès de la CNDP à réserver à la population berrichonne la primeur des informations relatives à ce projet. C'est pourquoi je souhaite vous inviter aux réunions de son comité de pilotage.

La préfecture nous a demandé de ne pas prendre directement contact avec les associations locales, notamment environnementales, avant que se tiennent les rencontres qu'elle organisera ; il en va de même des rencontres avec les concessionnaires RTE et Enedis, ainsi qu'avec toutes les autres parties prenantes. Je souhaite vous embarquer dans cette aventure, parce que nous avons beaucoup à apprendre de vous.

Mme Cyrielle Chatelain, rapporteure. Je viendrai avec plaisir.

M. Julien Lépine. Monsieur Bonnet, vous avez parlé de l'impact environnemental du *cloud* et des besoins qui en résultent. Nous avons beaucoup parlé des logiciels, mais le *cloud* est aussi un métier d'opération et de logistique. J'en profite pour remercier nos équipes qui travaillent au quotidien dans les *data centers* ; ils font tourner les infrastructures vingt-quatre heures sur vingt-quatre et sept jours sur sept pour servir nos clients.

Chez Amazon, nous avons un modèle mental qui est sans doute assez partagé : nous considérons le *cloud* comme le transport en commun de l'infrastructure. Les *clouds* ont besoin de plus d'infrastructures et plus de présence. Pour nous, l'efficacité énergétique est non seulement un impératif éthique important pour nos équipes, mais aussi un enjeu commercial. Un *data center* de type *cloud* moderne comme ceux que nous déployons est jusqu'à 4,1 fois plus efficace qu'un *data center* traditionnel. Tout un pan des travaux d'extension du numérique porte sur la modernisation des infrastructures.

Lors d'une audition que vous avez menée hier a été évoquée l'importante amélioration du nombre d'opérations de calcul par watt utilisé dans les *data centers*. Le PUE (*power usage effectiveness*, ou indicateur d'efficacité énergétique) est une norme internationale permettant de calculer cette amélioration : un *data center* traditionnel obtient un résultat légèrement supérieur à 1,6 PUE, ce qui signifie qu'il faut utiliser 1,6 watt d'énergie pour fournir 1 watt d'infrastructure ; AWS obtient un résultat de 1,15 PUE en moyenne mondiale et de 1,04 PUE en Europe. Nous dégageons donc un gain significatif.

Depuis de nombreuses années, nous travaillons également à fournir des infrastructures et des processeurs moins gourmands en énergie. Nous avons développé une puce, nommée Graviton, qui permet des gains d'énergie allant jusqu'à 60 % par rapport à une puce traditionnelle. Il est pour nous primordial de limiter le plus possible notre impact environnemental dans les infrastructures et les investissements.

AWS s'était engagée à produire une énergie 100 % renouvelable pour ses infrastructures de *cloud* en 2030 ; nous avons atteint cet objectif en 2023, avec sept ans d'avance. Nous nous sommes également engagés à atteindre la neutralité carbone en 2040, soit dix ans plus tôt que ce que prévoit l'accord de Paris.

Les modèles d'intelligence artificielle s'organisent selon deux parties : l'entraînement et l'inférence. Au cours des premières années de développement, la première était la plus consommée par les entreprises, mais la généralisation des agents conversationnels a rendu la deuxième plus intéressante et plus utilisée par les entreprises. Comme nous le faisons depuis vingt ans pour les infrastructures traditionnelles, nous avons développé des infrastructures

spécifiques afin d'optimiser leur consommation énergétique. Notre objectif est d'avoir la plus grande capacité de calcul pour la plus faible consommation de watts.

À ce jour, AWS opère en France quinze *data centers* en colocation et aucun en propre. Nous travaillons avec plusieurs entreprises françaises, contribuant ainsi à leur développement.

Mme Corine de Bilbao. Microsoft a pris de nombreux engagements environnementaux, dont celui d'être « carbone négatif » d'ici à 2030. Depuis la fin de l'année dernière, tous nos *data centers* sont alimentés par des énergies renouvelables, ce qui contribue beaucoup au développement de cette filière et notamment à ses acteurs français, avec lesquels nous avons développé une vingtaine de projets. Dans le monde, Microsoft dispose de 40 gigawatts de *power purchase agreements*, c'est-à-dire de contrats à long terme d'énergie renouvelable.

Nos engagements environnementaux portent également sur notre consommation d'eau. Nos nouveaux *data centers* bénéficient d'un approvisionnement en eau en circuit fermé. De plus, depuis fin 2024, 90 % des déchets des serveurs sont recyclés dans l'un de nos huit centres de recyclage, dont l'un est basé à Amsterdam.

S'agissant des *data centers*, nous fonctionnons selon un système de *leasing* dans les trois régions où sont installés nos serveurs : Paris, Marseille et Petit-Landau, dans l'est de la France, où nous nous sommes engagés, dans le cadre du sommet Choose France, à créer un *data center*. Ce site, d'environ 35 hectares, a fait l'objet de présentations publiques – je me suis moi-même rendue à Mulhouse en novembre dernier.

La construction d'un *data center* prend du temps ; en mobilisant une quarantaine de métiers, elle s'inscrit dans un écosystème local. Sa maintenance demande ensuite l'intervention de vingt à vingt-cinq métiers, contribuant ainsi à l'attractivité du territoire.

M. Philippe Limantour. Nos clients ont tous un modèle de consommation énergétique différent. Le premier enjeu en la matière étant la transparence, nous leur fournissons des tableaux de bord de suivi de leur consommation, notamment carbone, relatifs aux services qu'ils utilisent. Nous travaillons régulièrement avec eux pour déterminer comment améliorer leur consommation ; il s'agit de trouver l'équilibre entre l'innovation et la productivité. De nombreux protocoles sont en libre accès pour accompagner cette évolution, y compris au premier niveau, car cela commence souvent par le développement de logiciels plus frugaux.

En matière de consommation, nous faisons beaucoup de R&D ; notre rapport de puissance est d'environ 1,16 au niveau mondial. Les dernières générations de *data centers* fonctionnent avec un circuit fermé d'approvisionnement en eau.

Nous menons de nombreux travaux, notamment concernant l'intelligence artificielle. Nous avons développé des puces pour certaines phases de développement particulièrement consommatrices, équipées de mécanismes de refroidissement innovants : plutôt que d'installer un radiateur sur le processeur, qui est organisé en couches superposées, des micro-canaux sont intégrés à l'intérieur même du processeur. Grâce au liquide circulant ainsi en son sein, celui-ci diffuse moins de chaleur et nécessite moins de refroidissement.

Nous avons également consacré de nombreux travaux à l'allongement de la durée de vie, non seulement des postes, mais aussi des serveurs et de l'ensemble des systèmes. En faisant

ce que l'on appelle de la ségrégation, nous sommes capables de décomposer un serveur traditionnel et de regrouper entre eux différents équipements – les systèmes de stockage d'un côté, les puces graphiques de l'autre – pour lesquels les températures et les hygrométries doivent être maintenues à des niveaux différents. Plutôt que d'appliquer uniformément les niveaux correspondant aux équipements les plus exigeants, les adapter ainsi permet d'augmenter la durée de vie de tous les équipements et de réduire la consommation de matériaux et de terres rares – l'impact environnemental se mesure aussi en amont.

Une expérimentation est en cours concernant le bâti des *data centers* : des cloisons en bois remplacent les murs en béton. De plus, nous utilisons l'intelligence artificielle, avec des entreprises françaises, pour améliorer l'impact environnemental – en recourant à du béton moins carboné, par exemple – et découvrir de nouveaux procédés de fabrication. Nous aidons notamment nos clients à réduire leur consommation d'eau et d'énergie dans leurs processus de fabrication industrielle – dans l'utilisation de fours, notamment.

Alors que les chercheurs essayaient de trouver une solution depuis une quinzaine d'années, l'intelligence artificielle nous a aidés à créer, en quelques semaines, un liquide de refroidissement pour les *data centers* ne contenant pas de PFAS (substances per- ou polyfluoroalkylées). Nous avons aussi eu recours à l'IA pour aider un client à créer une batterie solide contenant 70 % de lithium de moins que les batteries traditionnelles, tout en étant plus performante.

Enfin, depuis le début, l'ensemble de la chaîne matérielle de Microsoft est diffusée en libre accès, dans le cadre de l'*Open Compute Project*. Les spécifications de tous nos serveurs, depuis le silicium jusqu'aux couches les plus hautes, sont en libre accès. Notre investissement dans la R&D est ainsi mis à la disposition de l'ensemble de la communauté, qui bénéficie des innovations. Toutes ces actions contribuent à améliorer l'impact environnemental.

M. le président Philippe Latombe. Le temps file, et nous n'aurons pas le temps d'aborder tous les sujets. Je vous remercie donc de bien vouloir nous transmettre par écrit vos réponses au questionnaire, ainsi que toute contribution susceptible d'éclairer nos travaux.

Nous n'avons pas parlé de Nitro, conçu par AWS, et nous serions intéressés par une note détaillée à son sujet. De même, nous aimerions savoir où sont stockées et comment fonctionnent les clés de chiffrement de Google et de Microsoft.

En matière de *cloud* souverain, Google et Microsoft ont développé des solutions avec des entreprises françaises, mais le modèle d'AWS est totalement différent : vous avez annoncé un *cloud* AWS souverain et nous aimerions avoir des informations écrites à ce sujet, afin d'écarter tout soupçon de « *souverain-washing* ». *Quid* du *kill switch* si les États-Unis vous demandaient de cesser de fournir vos services ? La nationalisation de cette société de *cloud* AWS souverain – à tout le moins celle des murs et des infrastructures – est-elle prévue dans les contrats ? Comment tout cela fonctionnera-t-il en pratique, au cas – improbable selon Microsoft – où surviendrait un *kill switch* généralisé ?

Mme Cyrielle Chatelain, rapporteure. Pour rester sur le sujet du *cloud* AWS souverain, la question du président sur la nationalisation des murs se pose également s'agissant des contrats, car les salariés, basés en Europe, signent un contrat de travail avec AWS. Je vous remercie d'intégrer cette dimension dans la note juridique que vous nous ferez parvenir, afin que nous ayons connaissance de l'ensemble de la chaîne de décision.

Nous avons beaucoup parlé de données chiffrées. Toutes les données que vous stockez – les échanges d'e-mails, les Google docs, etc. – sont-elles chiffrées ? Dans l'affirmative, par qui le sont-elles ? Qui possède la clé de chiffrement ? Les équipes françaises et européennes des infrastructures souveraines dites hybrides – S3NS ou Bleu – ont-elles accès au code ?

Quelle est la fréquence des mises à jour pour les *clouds* de ce type ? Sont-elles effectuées par vos équipes, qui prennent la main sur l'infrastructure, ou envoyez-vous des éléments de code aux équipes françaises, qui les installent ? Si une mise à jour n'est pas effectuée, combien de temps faut-il pour qu'une éventuelle faille soit identifiée et exploitée dans le cadre d'une cyberattaque ? L'Anssi estime qu'il faut en moyenne cinq jours ; d'autres professionnels nous ont parlé de vingt-quatre heures.

M. le président Philippe Latombe. Dans les notes que vous nous transmettrez, nous voudrions également que vous distinguiez le chiffrement au repos et celui en traitement, qui sont très différents. Nous serions intéressés par vos solutions de chiffrement homomorphiques, si vous en utilisez.

M. Frédéric Geraud de Lescazes. Thales dit publiquement qu'il a accès au code ; l'Anssi vous l'a confirmé, et je vous le confirme également. Dans le cas contraire, nous n'aurions pas atteint le niveau de confiance nécessaire pour obtenir la certification SecNumCloud.

S'agissant des mises à jour, nous utilisons une zone de quarantaine, c'est-à-dire un serveur sécurisé sur lequel Google dépose soit une mise à jour, soit un nouveau service. En effet, comme l'a annoncé Thales, des services vont se surajouter, car la gamme d'offres va s'enrichir progressivement, notamment avant la fin de l'année avec toute la partie intelligence artificielle de Google Cloud Platform. Une fois que Google Cloud a effectué ce dépôt, nous ne savons pas ce qui se passe, car nous tenir à distance est le principe même de SecNumCloud. Nous n'avons pas le droit d'entrer, ni même de sonner, dans cette maison dont nous détenons pourtant 5 % ; avant d'accepter notre participation, nous avons été mis à nu et examinés sous toutes les coutures…

Mme Cyrielle Chatelain, rapporteure. Vous devez y trouver un intérêt, j'imagine !

M. Frédéric Geraud de Lescazes. Oui. L'intérêt, c'est que nous sommes le seul *hyperscaler* en mesure de dire à ses clients : « Vous voulez une certification SecNumCloud ? Ce ne sera pas avec nous, mais nous savons faire, avec les mêmes architectures et les mêmes logiciels. » Les clients peuvent ensuite déterminer la sensibilité de leurs données et répartir en temps réel la charge de travail à des équipes d'ingénieurs qui maîtrisent le sujet et qui travaillent avec la même console d'administration. C'est là que réside la puissance du modèle S3NS : chaque client peut modifier le niveau de sensibilité de ses données. Ensuite, Thales procède à son expertise.

Comme l'Anssi vous l'a dit lors de son audition, les mises à jour sont continues – plus il y a de services, plus il y a de mises à jour. De même que l'on parle d'un continuum de cyberattaques, il existe un continuum de mises à jour. Thales a dimensionné ses équipes d'ingénieurs pour faire face à cet enjeu. Combien d'acteurs disposent d'équipes d'ingénieurs suffisamment expérimentées et nombreuses pour endosser cette charge de travail ? Ce faisant, Thales fait croître sa courbe d'apprentissage ; il voudra probablement suivre d'autres envies.

Dans le modèle S3NS, Thales a placé autour de toutes nos solutions des surcouches de sécurité, auxquelles nous n'avons pas accès. Enfin, il a pris publiquement l'engagement de maintenir le modèle S3NS pendant douze mois en cas de problème de mise à jour.

Mme Cyrielle Chatelain, rapporteure. Nous avons entendu plusieurs témoignages concernant les engagements de Thales.

Vous n'avez pas répondu à ma question : combien de temps faut-il pour qu'une éventuelle faille de sécurité soit identifiée et exploitée ?

M. Frédéric Geraud de Lescazes. Il existe différents types de vulnérabilités. Celles qu'on appelle « *zero day* » nécessitent une réponse très rapide. Lorsque les équipes de Google découvrent une telle faille dans nos solutions ou nos services, elles apposent un patch et le placent dans la zone de quarantaine. Ensuite, Thales décide seul de la mise en production de la mise à jour, éventuellement en mobilisant davantage d'ingénieurs pour l'accélérer s'il considère que réparer cette faille est crucial. Nous n'avons pas la main sur cette décision.

Mme Cyrielle Chatelain, rapporteure. Je suppose qu'une faille *zero day* implique un risque immédiat pour la continuité du service.

M. Frédéric Geraud de Lescazes. Tout à fait.

Mme Corine de Bilbao. Je ne voudrais pas que cette commission reste sur l'impression qu'il n'y a pas de concurrence. Cette concurrence est forte, tant concernant le SecNumCloud que le *cloud* public, même si Google se positionne en tant que *challenger*.

Cette concurrence est saine et Bleu y contribue, avec un modèle un peu différent, dépourvu de liens capitalistiques. Du reste, Bleu est le seul acteur à proposer à la fois le *cloud* et la suite collaborative Office.

M. Philippe Limantour. Depuis l'origine des développements de Microsoft, 100 % des données sont systématiquement chiffrées, qu'elles soient au repos ou en transit.

Les clés de chiffrement font l'objet d'une hiérarchie. Au sommet se trouve la possibilité pour le client de gérer sa propre clé, dont il est le seul détenteur – s'il perd sa clé, il perd ses données. Les clés peuvent être stockées dans un coffre muni d'un mécanisme de calcul confidentiel, provenant de l'un de nos trois fournisseurs ; ces mécanismes nous empêchent physiquement et techniquement d'accéder à la clé. Personne, chez Microsoft, n'a accès ni aux données ni aux plans de données : des mécanismes d'isolation systématique sont installés dans tous nos serveurs.

Le calcul confidentiel a été inventé par les laboratoires de recherche de Microsoft en 2014. Nous avons des services opérationnels dans Azure depuis 2017 ; ils ne s'appuient pas sur un chiffrement homomorphique, mais sur une racine de confiance matérielle. Depuis 2017-2018, l'ensemble des spécifications – tous nos codes d'attestation et de signature associés à ces services – sont placées dans un consortium de calcul confidentiel *open source*.

Au-delà du transit et du repos, l'ensemble des mécanismes de traitement sont chiffrés, protégeant ainsi les codes logiciels de nos clients – la propriété intellectuelle et l'ensemble des traitements. Seul le bus de traitement du processeur a accès à la donnée en clair.

Un mécanisme protège la chaîne d'approvisionnement des attaques : des vérifications sont faites avant de libérer la clé et de donner accès aux traitements ; si la version du logiciel ou du *firmware* du client n'est pas celle qui est prévue, le système se bloque. Un système de *cloud* est complexe : les deux tiers de nos services sont basés sur des logiciels *open source*.

S'agissant des mises à jour, les attaquants sont de plus en plus efficaces : les vitesses d'exploitation des vulnérabilités sont variables, mais de plus en plus rapides. Ces attaques sont de plus en plus complexes et nécessitent une organisation en « petits pas » : plutôt qu'une porte grande ouverte, ce sont plusieurs éléments qui doivent être activés. Avant de recourir à des mises à jour, il existe des mécanismes de défense en profondeur permettant de bloquer l'un des maillons d'une chaîne de dix, quinze ou vingt petits pas, pour bloquer les attaques. Ainsi, ce n'est pas parce qu'on trouve une vulnérabilité dans un code qu'elle est exploitable. Cette chaîne d'actions complexe est défendable sans qu'il soit nécessaire de procéder à la mise à jour du logiciel.

Je ne dispose pas des détails de l'implémentation de Bleu. En l'absence de mise à jour – ce qui est le cas dans de nombreux *data centers* traditionnels – les systèmes ne s'arrêtent pas du jour au lendemain. Les délais avant que les risques deviennent suffisamment importants se compteraient en semestres.

Mme Cyrielle Chatelain, rapporteure. Vous avez parlé du sommet de la hiérarchie des clés de chiffrement, qui correspond au chiffrement par le client lui-même et au stockage dans des espaces sécurisés. Afin d'avoir une idée générale, quelle est la proportion des chiffrements effectués par Microsoft, des chiffrements effectués par les clients eux-mêmes mais non sécurisés et des chiffrements effectués par les clients eux-mêmes correspondant au sommet de la hiérarchie ?

M. Philippe Limantour. Le client peut chiffrer 100 % de ses données stockées. Les données accessibles sont les données stockées ; les clés de chiffrement sont disponibles pour l'ensemble de nos services utilisables par nos clients. Les services Azure Local permettent d'avoir accès aux mêmes outils que ceux proposés par Bleu, mais en propre ; les opérateurs de Microsoft n'y ont pas accès. Des mécanismes de double chiffrement sont également à la disposition de nos clients. Enfin, il existe un mécanisme de calcul confidentiel.

Mme Cyrielle Chatelain, rapporteure. Globalement, quel est le pourcentage de vos clients qui utilisent ces différents types de chiffrement ?

M. Philippe Limantour. Je ne connais pas ce pourcentage. Ce service est gratuit pour nos clients, et nous leur conseillons d'y recourir. Il figure dans notre architecture de souveraineté, et des mécanismes permettent de l'appliquer systématiquement à tous les services utilisés par le client. Outre les clés de chiffrement, d'autres mécanismes de protection interviennent ; ainsi, il est possible de ne pas exécuter un service si certaines conditions ne sont pas remplies.

M. Julien Lépine. Présenter Nitro serait en effet beaucoup trop long, mais je vais vous donner quelques éléments d'information ; nous vous transmettrons des éléments plus détaillés par écrit.

Par défaut, Nitro permet à tous nos clients, quand ils lancent gratuitement des infrastructures, de bénéficier de l'isolation de leurs données, qu'elles soient en traitement, en transit ou en repos ; celles-ci sont soit chiffrées, soit complètement isolées, sans aucune possibilité d'accès pour les opérateurs.

Pour tous nos clients, 100 % des données sont chiffrées gratuitement. Le chiffrement est actif par défaut lorsque vous utilisez un service AWS, par le biais de clés gérées par AWS. Je ne connais pas la proportion de clients qui opèrent eux-mêmes des HSM (*hardware security module*) – autrement dit, des boîtiers de sécurité.

Vous nous avez interrogés au sujet de notre modèle de souveraineté, qui diffère de celui des autres entreprises. Nous avons formé des ingénieurs et effectué un transfert de technologie vers les équipes présentes sur le sol européen ; elles ont accès à 100 % du code source et sont capables de le déployer et de le maintenir dans la durée. Cette façon de faire figure dans les statuts de l'entreprise.

Nous avons créé une entreprise qui gère les clés de sécurité sur le sol européen. Du point de vue technique, organisationnel et de gouvernance, nous nous sommes assurés que les droits allemand et européen seraient les premiers à être appliqués.

Vous avez posé la question de la fréquence des mises à jour. Nous proposons plus de 200 services, dont plus d'une centaine concernant le *cloud* souverain européen, ce qui implique de très nombreuses mises à jour – nous en effectuons beaucoup, chaque jour. Certaines d'entre elles sont des mises à jour critiques, nécessaires pour garantir la sécurité des infrastructures. Parallèlement, nous nous attachons à maintenir les capacités opérationnelles des équipes locales, qui doivent être en mesure de comprendre ce qui se passe, de procéder à des audits et d'apporter cette garantie.

Nous n'avons pas de chiffrement homomorphique largement disponible – nous aimerions pouvoir vous répondre par l'affirmative…

Les réponses aux vulnérabilités sont de plus en plus rapides : elles sont quasiment apportées dans la journée. Un système de *cloud* n'est pas juste une infrastructure ; l'une des véritables différences avec les infrastructures *on-premise*, c'est que nous analysons chaque jour 400 000 milliards de flux réseau. L'intérêt, avec une infrastructure comme AWS, c'est de ne pas être tout seul avec sa machine face aux vulnérabilités. Nous travaillons avec les autorités européennes et avec l'Anssi, afin de bénéficier du meilleur niveau de qualité en matière de sécurité. Ce faisant, toute entreprise, même une PME qui n'a pas les moyens de financer des équipes de sécurité renforcée, bénéficie de cet investissement. Ainsi, nous considérons le *cloud* à la fois comme un enjeu et comme un accélérateur de la sécurité.

M. Frédéric Geraud de Lescazes. L'autonomie stratégique n'est pas un sujet nouveau. Avec Thales, nous avons trouvé en 2019 un accord sur le chiffrement ; nous recherchions un système de chiffrement, qu'on appelle aujourd'hui EKM pour « *external key management* », c'est-à-dire gestion externalisée des clés, et Thales a été le premier à nous fournir ce service. L'aventure de S3NS est partie de là.

Désormais, tous nos clients ont accès à la solution EKM, qui leur permet de choisir où déposer leurs clés : chez nous ou chez un partenaire – le premier d'entre eux, en France, étant Thales, mais il en existe d'autres dans le reste du monde. Ils ont ainsi la garantie que nous ne pouvons y accéder et lire leurs données.

Mme Cyrielle Chatelain, rapporteure. Vous parlez de vos clients professionnels, mais Google propose ses services à un public plus vaste.

M. Frédéric Geraud de Lescazes. Je parlais bien de Google Cloud Platform, qui propose des services aux entreprises. Nous proposons une autre solution, nommée Client-Side Encryption – « chiffrement du côté du client » –, pour le grand public. Cette technologie, qui n'existe pas chez nos concurrents, a déjà été examinée par différents experts de la place.

M. le président Philippe Latombe. Merci beaucoup. Nous lirons avec intérêt les éléments que vous voudrez bien nous transmettre sur les divers sujets que nous n'avons pas eu le temps d'évoquer.

La séance s'achève à dix-sept heures trente.

Membres présents ou excusés

Présents. – M. Nicolas Bonnet, Mme Cyrielle Chatelain, M. Philippe Latombe, M. Hervé Saulignac, M. Aurélien Taché

Excusé. – Mme Isabelle Rauch