ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Mission d'information de la Conférence des Présidents « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Mardi
13 avril 2021
Séance de 13 heures

Compte rendu n° 59

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Laurent Degré, président-directeur général de la société Cisco Systems France et de M. Bruno Bernard, directeur des affaires publiques de la société Cisco Systems France

La séance est ouverte à 13 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le Président Jean-Luc Warsmann. M. Laurent Degré est président-directeur général de la société Cisco Systems France, M. Bruno Bernard, son directeur des affaires publiques.

Cisco Systems est une entreprise informatique américaine fondée en 1984 et spécialisée dans les matériels informatiques et les solutions de cybersécurité. Vous avez un large champ d'action, qui devrait nous permettre de balayer un grand nombre de sujets, des enjeux cyber à l'identité numérique, en passant par la transformation numérique des entreprises.

M. Philippe Latombe, rapporteur. M. le président-directeur général, j'aimerais d'abord vous interroger sur votre acception de la notion de souveraineté numérique. Cette notion revêt une grande diversité de définitions. Que recouvre pour vous ce concept, que l'on rapproche parfois d'une forme d'autonomie stratégique et décisionnelle, et de quelle façon les politiques menées par les États peuvent-elles ou doivent-elles évoluer pour mieux intégrer cette composante stratégique ?

En second lieu, je voudrais que nous échangions sur l'écosystème des entreprises du numérique. Cisco mène des activités variées, dans des domaines comme le matériel informatique, mais aussi la cybersécurité. Comment vous positionnez-vous sur le marché européen ? Comment appréhendez-vous notamment le sujet de l'identité numérique, sur lequel nous travaillons au sein de cette mission d'information ?

De façon plus générale, je voudrais vous entendre sur les attentes de vos clients, dont certaines entreprises françaises font partie. À l'occasion de cette crise sanitaire durable, avez-vous observé des changements dans leur comportement numérique ? Peut-on dire que la crise sanitaire a accéléré leur sensibilisation face au risque cyber, par exemple ? À l'inverse, comment peut-on expliquer les difficultés que certaines entreprises continuent de rencontrer à l'heure actuelle pour se numériser ? Quelles seraient selon vous les solutions ?

Enfin, je voudrais évoquer la question de la formation aux compétences numériques. Quel regard portez-vous sur le niveau du système de formation français à cet égard ? Un Campus Cyber est par exemple en cours de déploiement, visant à rassembler un vivier d'acteurs de pointe. Comment jugez-vous ces différentes initiatives mises en œuvre en France ? Existe-t-il leur équivalent dans les pays au sein desquels vous êtes présents ?

M. Laurent Degré, président-directeur général de la société Cisco Systems France. Je voudrais en premier lieu revenir sur ce qu'est Cisco, ce que nous faisons et ce que nous ne faisons pas, ce qui peut être important pour la suite des questions que vous avez abordées. Cisco est comme vous l'avez précisé une société née en 1984. Notre métier est simple : il s'agit de connecter les applications, les équipements, les personnes, de transporter les flux d'information et de les sécuriser. L'entreprise compte 77 000 salariés dans le monde, dont 700 en France, un certain nombre d'entre eux étant des chercheurs. Ces derniers ont

notamment intégré la société anciennement appelée Sentryo, une pépite de la cybersécurité dans le monde industriel.

Notre métier n'est pas le commerce de la donnée : nous la transportons et la sécurisons. La cybersécurité est en revanche notre métier, du point de vue de l'outillage, des solutions logicielles et matérielles, ainsi que de la manière dont nous développons nos produits, dont nous interagissons avec nos prestataires et dont nous intégrons la sécurité de la conception à la fabrication.

Notre modèle de vente est exclusivement indirect. Tout ce que nous fournissons en termes de technologie est intégré, distribué, déployé et opéré par nos partenaires. Nous avons 1 200 partenaires français, dont certaines grandes entreprises comme Atos, Thales, Orange ou SFR, ainsi que tout un réseau de distributeurs à valeur ajoutée. Notre *business model* s'appuie donc sur les acteurs de confiance de l'écosystème français.

Nous contribuons à la formation aux métiers du digital dans l'écosystème, en formant 30 000 personnes par an – demandeurs d'emploi, formations certifiantes, cursus de formation intégrés (dans les IUT notamment) dans l'Éducation nationale.

La souveraineté numérique est un mouvement que nous observons en France, et auquel nous sommes très sensibles. Il se manifeste également au niveau global et dans de très nombreux pays. Nous y sommes très attentifs. Encore une fois, notre métier n'est pas de conserver ou de commercer des données, mais nous nous intéressons aux problématiques de souveraineté.

L'autonomie est un premier aspect, mais le contrôle des données est également très important. Parmi toutes ces plateformes de type *cloud*, nous proposons la solution Webex. La souveraineté renvoie à la notion de frontières, alors que le *cloud* et Internet de manière générale ont été conçus en s'affranchissant de ces règles. Nous devons néanmoins absolument disposer de la capacité de réglementer, de nous adapter à ces problématiques, pour conserver le contrôle des données au niveau d'un pays, mais aussi d'une entreprise.

Il convient de distinguer souveraineté numérique et protectionnisme. Nous pensons qu'il est important d'utiliser la technologie telle qu'elle est mise en place par les acteurs du marché, dont Cisco, tout en créant des garde-fous réglementaires et les processus nécessaires. Une fermeture ou un cloisonnement ne peut pas répondre à l'ensemble des questions. Bénéficions de la technologie, travaillons avec des acteurs tels que l'ANSSI en France, qui est très en avance en termes de recommandations et de réglementation. C'est un travail qui doit se faire avec les industriels. Mettons les bons outils en place pour faire en sorte que tout cela se passe sous un contrôle, ou du moins une protection des États.

Reste une dimension importante, celle de l'industrialisation. Selon les pays, les demandes que recouvre la notion de souveraineté numérique sont bien souvent différentes. On parle de localisation des données dans un cas, de centre de données localisées dans un autre, de cybersécurité ailleurs, ou encore de possibilités de contrôler et de débrancher des applications. L'aspect industriel est extrêmement important pour des acteurs comme Cisco ou d'autres. Élaborer une solution pour chaque pays est très compliqué si l'on veut concilier l'innovation, l'aspect industriel, la capacité à proposer des applications et des services bénéficiant de cette innovation, tout en répondant aux réglementations.

M. Bruno Bernard, directeur des affaires publiques de la société Cisco Systems France. En matière de souveraineté, la question du droit applicable aux données est également essentielle. Si nous voyons des demandes de localisation émaner de beaucoup de pays, nous pensons que la vraie question de la souveraineté se joue sur le droit applicable. Tout l'enjeu est de trouver un modèle permettant aux États de garantir une sécurité des données de leurs citoyens et de leurs entreprises, tout en permettant à ces derniers de continuer à bénéficier des meilleures solutions technologiques disponibles. L'entente est donc nécessaire entre les États. Nous y incitons, que ce soit aux États-Unis ou ailleurs dans le monde, pour que des formes juridiques soient trouvées pour garantir ces transferts de données.

M. Philippe Latombe, rapporteur. Vous parlez de la manière de trouver une réglementation applicable. Comment faire dans le contexte actuel où il existe une extraterritorialité forte des règles américaines ? Comment assurer aux Européens que les données hébergées dans le *cloud* ou utilisées dans des algorithmes sont bien localisées et opérées sur le territoire européen, sans possibilité de prise de la part de la réglementation américaine ? Les clauses contractuelles-types telles que la localisation des données dans des serveurs européens et le chiffrement sont-elles suffisantes ? Que ferait par exemple Cisco si une agence américaine lui demandait de fournir des informations ?

M. Laurent Degré. Vous faites référence au *Cloud Act*.

M Philippe Latombe, rapporteur. Ce n'est pas la seule loi dans ce domaine, même si elle est celle qui a fait le plus de bruit avec *Schrems* II. Il existe des règles extraterritoriales américaines assez fortes en dehors du *Cloud Act*.

M. Laurent Degré. Nous sommes une société américaine, sujette à ces lois.

M. Philippe Latombe, rapporteur. C'est bien pour cette raison que je vous pose cette question.

M. Laurent Degré. Même si nous sommes une filiale française du Groupe, nous sommes soumis à ces contraintes. Un processus existe en la matière, que j'invite M. Bruno Bernard à rappeler.

M. Bruno Bernard. L'extraterritorialité est malheureusement un concept à la mode en ce moment. Beaucoup de règlements sont extraterritoriaux en matière numérique : le RGPD est, par exemple, extraterritorial de fait. C'est toute la problématique de l'application du droit dans des sphères qui ne sont pas traditionnelles. Les sollicitations que nous sommes susceptibles de recevoir d'agences gouvernementales ne se limitent pas aux États-Unis.

Pour ce qui concerne le *Cloud Act* précisément, nous rappelons que son application suppose la demande d'un juge, sollicité par une agence gouvernementale.

Notre processus est standard, mais relativement fort. La question se pose de savoir où se trouve la donnée. La plupart du temps, elle est chez le client. Nous demandons donc que l'agence ou le juge s'adresse directement à notre client. Si la demande est adressée directement à Cisco, nous en notifions le client, pour éviter toute rupture de confiance. Il est possible qu'une décision judiciaire nous l'interdise, auquel cas nous la contestons devant la juridiction compétente.

Ensuite, nous communiquons des données aux autorités qui ont réellement compétence. Dans le cas du *Cloud Act*, par exemple, nous ne communiquons pas de données

en l'absence de la décision d'un juge. Nous cherchons également toujours à réduire la portée de la requête au strict minimum correspondant à la demande.

Dans la configuration où la demande légale d'un gouvernement nous mettrait dans une situation de conflit de lois entre deux législations ayant autorité sur les données (par exemple, entre un pays européen et les États-Unis), nous irions devant un juge pour réfuter cette demande, en invoquant les traités d'assistance judiciaire mutuelle existants.

Je tiens également à signaler que nous publions un rapport de transparence (*transparency report*), dans lequel nous listons les demandes de transmissions de données par pays. Elles sont très peu nombreuses, notamment depuis l'entrée en vigueur du *Cloud Act*.

M. Philippe Latombe, rapporteur. Comment percevez-vous le marché européen du numérique ? S'agit-il d'un marché mature, ou encore adolescent ? Je voudrais que l'on sépare pour traiter cette question la partie relative au numérique de manière générale et celle de la cybersécurité en particulier, car il existe peut-être deux types de maturité différents.

M. Laurent Degré. Il existe plusieurs aspects dans cette question : la maturité digitale de manière globale, celle des éditeurs et la question de notre force de frappe en Europe.

Nous avons la chance en France de disposer de beaucoup de champions dans le domaine numérique – Atos, Thales –, de champions en matière de cybersécurité, qui nous sont enviés, d'une agence de régulation, d'excellents cursus de formation. Je n'ai donc pas le sentiment que nous ayons des lacunes en matière de cybersécurité. Nous sommes peut-être derrière les États-Unis concernant les éditeurs capables de fournir du software et des solutions dans leur globalité pour servir l'Europe. Du point de vue de l'intégration, des compétences et de l'écosystème, nous avons en revanche quelque chose de très fort en France.

Cybermalveillance est par exemple une excellente initiative, dont nous faisons d'ailleurs partie. De même, nous officialiserons notre contribution au Cyber Campus. Il s'agit de la meilleure des réponses. Nous ne sommes pas du tout en retard, et disposons du bon écosystème et des bons acteurs pour pouvoir avancer sur la cybersécurité.

Il existe de nombreux classements relatifs à la maturité digitale des entreprises de manière générale, que nous serions heureux de partager avec vous. Pour faire simple, nous pouvons formuler deux constats pour la France :

– nos grands groupes sont bien équipés : nous avons vu, dans la crise du Covid, qu'ils étaient capables de réagir ;

– en revanche, il existe certainement un déficit, par rapport à d'autres pays, parmi les PME et ETI, en termes d'acculturation, de formation et de perception du numérique en général et de ce qu'il représente en matière de valorisation de l'entreprise, de relation client, d'amélioration des modes de fonctionnement et de performance industrielle ou économique. En matière de cybersécurité en particulier, nous avons un travail d'éducation à mener. Je considère que la cybersécurité doit être un investissement, plutôt qu'un coût de fonctionnement. Protéger vos données et vos salariés revient à valoriser votre entreprise. Une accélération de l'acculturation, de la prise de conscience et de la gouvernance est nécessaire sur le sujet.

M. Philippe Latombe, rapporteur. Est-ce lié au mouvement d'externalisation de l'informatique dans les entreprises ?

M. Laurent Degré. Les sujets sont selon moi décorrélés. Le numérique est de toute façon omniprésent, comme nous l'avons vu dans la crise sanitaire. Le Covid est ni plus ni moins qu'un accélérateur de la transformation. Le digital est partout, dans l'Internet des objets, la relation client, le management, l'interaction avec les fournisseurs. Qu'il soit dans le nuage ou non, beaucoup d'activités se numérisent de toute façon, ce qui conduit à une augmentation de la surface d'attaque. La prise de conscience est donc nécessaire, indépendamment de la question de l'externalisation.

M. Philippe Latombe, rapporteur. Les plans européen et français de relance sont-ils une bonne manière d'aborder le sujet ? Le financement n'est-il à l'inverse que la partie émergée de l'iceberg, et y a-t-il d'autres champs (comme l'éducation) à investir d'abord ?

M. Laurent Degré. Ces programmes d'investissement sont bons. Le plan de relance européen et les investissements prévus en France constituent une démarche excellente. Son orchestration est une question d'écosystème.

L'Éducation nationale doit faire partie intégrante du processus. La cybersécurité est un marché en constante évolution. On parle d'un poids de la cybercriminalité de plus de 4 000 milliards d'euros dans le monde, ce qui donne une idée de sa puissance, si l'on rapporte ce chiffre au PIB. Il s'agit d'un processus continu, qui évolue. L'éducation, quelles que soient les filières, doit être au cœur des investissements. À côté des aspects technologiques et de formation pour les industriels, l'éducation doit être un pilier de la démarche. Nos étudiants, nos élèves, ne sont pas toujours conscients de ce qu'ils font, ce qui peut se traduire par la suite dans l'entreprise. L'éducation est donc selon moi un point critique. Nous essayons autant que possible de contribuer, au travers de beaucoup d'initiatives, à ces aspects d'acculturation et de formation, mais ce n'est pas suffisant : il faut faire encore beaucoup plus.

M. Bruno Bernard. La clef est de faire pénétrer les réflexes numériques dans la vie de tous les jours. Lorsque vous prenez un crédit bancaire, que vous vous assurez, que vous vous engagez dans votre vie de tous les jours, on pourrait imaginer un volet numérique, et un volet relatif à la cybersécurité, puisque ces questions peuvent avoir des impacts tout à fait concrets pour les entreprises, mais aussi pour les particuliers.

Les plans de relance et d'investissement sont la bonne manière de faire, mais le moment est venu de pleinement infuser ces problématiques dans le quotidien des entreprises et des citoyens.

M. Philippe Latombe, rapporteur. Comment inscrire le numérique et la cybersécurité dans les formations ? Faut-il créer des filières spécifiques ? Doit-il s'agir uniquement de filières d'excellence, d'ingénieurs ? Certaines personnes auditionnées nous ont expliqué que nous manquions également de techniciens, de personnes capables de coder, de « mettre les mains dans le cambouis », et qu'il existait un besoin de formations de niveau BTS ou IUT sur ce type de sujets. Comment faire pour trouver des personnes ?

M. Laurent Degré. La formation de spécialistes existe d'ores et déjà. Nous n'avons pas de problème de formation d'experts, mais l'acculturation et l'infusion de principes fondamentaux des bonnes pratiques du digital dans l'ensemble des filières sont essentielles. Il me semble que cette approche doit être aussi évaluée.

M. Bruno Bernard. Cisco faisait, à l'époque où les interventions physiques étaient possibles, de l'acculturation pour des collégiennes dans le département des Hauts-de-Seine, en

leur montrant comment fonctionnait un réseau et quel était le parcours de la donnée. Nous pensons que c'est à cette période de la vie, qu'il faudrait former les personnes à se servir d'un smartphone, à publier sur les réseaux sociaux, à savoir quels types de données partager. À notre avis, c'est à ce moment que l'on peut former des personnes qui soient totalement *digital natives*. Ils savent pour le moment se servir des applications, mais ignorent comment elles fonctionnent et quels sont les tenants et aboutissants de cette économie numérique. Nous recommandons donc des interventions au niveau du collège, qui ne soient pas du tout spécialisées, mais au contraire touchent l'ensemble de la population de cet âge.

M. Philippe Latombe, rapporteur. Selon vous, la crise sanitaire et le recours au numérique, tel que nous l'avons vécu de manière forcée, et tel qu'il s'est prolongé depuis un an, changent-ils la manière de fonctionner des entreprises en interne, par exemple pour les réunions, les pratiques de management ? La situation les a-t-elle renvoyés à un mode projet ? Cette question est valable pour les entreprises, mais également pour les administrations, si vous en avez une vision.

M. Laurent Degré. Indéniablement, cette crise sanitaire, qui a forcé beaucoup d'entreprises à accélérer leur digitalisation, a changé les comportements. Prenons l'exemple de ce que nous appelons le travail hybride : la relation au travail et au lieu physique a changé. Le digital, la connectivité, le *cloud* ont été un moyen de résilience économique pour les entreprises.

Nous avons vu plusieurs étapes. La première était celle de l'équipement, parfois sans garde-fous, sans acculturation, avec parfois des erreurs. Nous l'avons vu avec l'utilisation de certaines applications de collaboration, qui ont été bannies par certains États. Nous revenons aux thèmes de la formation, de l'acculturation, des bonnes pratiques, du choix des bons partenaires. Je pense que nous sommes maintenant dans une phase où le digital est plus important qu'auparavant, parce qu'il change la relation au travail, les modes de fonctionnement, mais qu'il y a encore beaucoup à faire sur les bonnes pratiques.

M. Bruno Bernard. Pour ce qui est des administrations, nous constatons un changement d'attitude, mais il demeure certains blocages, notamment vis-à-vis de l'utilisation d'outils de vidéoconférence. Nous avons essayé de porter ce message auprès du ministère de l'éducation nationale, pour venir en aide aux professeurs et aux élèves consignés chez eux. La volonté existe, mais cela reste compliqué, car non encore tout à fait naturel.

M. Philippe Latombe, rapporteur. Au-delà de la numérisation, les modes de fonctionnement des entreprises ont-ils durablement changé, en termes de gestion en mode projet, de rapidité, de capacité d'évolution, d'agilité ? Les entreprises et les administrations ont-elles compris que le temps n'était plus aussi long qu'auparavant, qu'il fallait se préparer à quasiment tout, que l'incertitude était chaque fois présente ?

M. Laurent Degré. Votre question n'est pas évidente, M. le rapporteur.

M. Philippe Latomb, rapporteur. Lorsqu'ils recourent à vos services, demandent-ils que leur système puisse évoluer presque instantanément, en fonction de ce qui arrive ? Veulent-ils se laisser en permanence des portes ouvertes dans les services qu'ils vous demandent ?

M. Laurent Degré. Le numérique, l'accès à ces applications, à ces outils, est critique pour la pérennité du fonctionnement des entreprises, leur vélocité. Il s'agit d'un sujet très

important pour nous, sur lequel nous possédons beaucoup d'études que nous pourrons vous partager.

En matière de relation au travail, il y a la notion de temps long et de temps court, celle de résilience, apportée par le digital. Dans les entreprises comme les administrations, l'utilisation du digital et de ses outils change la relation au travail et au management. Lorsque vous travaillez à distance, comme nous sommes en train de le faire, les notions d'horaire, de lieu physique et de relation avec votre manager changent. On est obligé de faire travailler les personnes sur un mode de confiance, d'objectifs. Je pense que cela est en train de révolutionner les modes de fonctionnement dans certaines entreprises. La technologie est une chose, mais les modes de gouvernance et la manière dont elle est utilisée pour le bien de l'entreprise ou de l'administration en est une autre. La relation hiérarchique n'est plus la même qu'auparavant en raison de l'utilisation de ces outils. J'ignore si je réponds à l'ensemble de vos questions, mais c'est un point qui me vient à l'esprit et qui est extrêmement important.

M. Philippe Latombe, rapporteur. Vous êtes acteur de l'identité numérique. Comment voyez-vous ce sujet émerger ?

M. Bruno Bernard. Nous avions participé à la mission d'information de l'Assemblée nationale sur le sujet de l'identité numérique.

M. Philippe Latombe, rapporteur. Elle était menée par M. Jean-Michel Mis, qui participe également à la présente mission.

M. Bruno Bernard. Nous avions positionné ce que nous percevions comme le futur de l'identification numérique d'une personne. Cela correspond tout à fait à notre démarche de cybersécurité. Nous préconisons une augmentation du nombre de critères de vérification de l'identité de la personne, de son comportement en ligne et de son positionnement géographique, grâce à des outils liés aux smartphones notamment. Nous sommes très favorables à une sécurité fondée sur le principe *zero trust* : il ne suffit pas de s'identifier une fois, et la posture doit être cohérente pour que l'identité des personnes sur Internet soit garantie.

Nous considérons qu'il revient aujourd'hui aux États et aux organisations internationales de prendre la main sur la définition de l'identité numérique – comme l'a fait l'Union européenne, et comme, me semble-t-il, le gouvernement français s'est engagé à le faire prochainement.

M. Philippe Latombe, rapporteur. Comment percevez-vous le retard pris sur le sujet ? Le rapport date d'il y a quelque temps. Or, nous n'avons fondamentalement pas avancé, même si la carte nationale d'identité électronique, réceptacle de l'identité numérique, arrivera prochainement. Nous n'avons pas grand-chose sur l'identité numérique pour l'instant, à part France Connect, qui n'a pas évolué. Comment percevez-vous ce retard ?

M. Bruno Bernard. J'ai cru comprendre que France Connect faisait partie des sujets qui seraient accélérés dans les quatre cents derniers jours, ainsi que Mme la ministre, Amélie de Montchalin, l'a récemment indiqué.

Malheureusement, la France aime prendre son temps. Nous sommes donc fréquemment un petit peu en retard, car nous souhaitons voir comment les choses se passent,

pour bien les mesurer. Notre retard n'est pas irrattrapable, mais comme souvent, en matière de numérique en particulier, il serait bon de ne pas laisser ce retard se creuser.

M. Philippe Latombe, rapporteur. Vous êtes une entreprise qui travaille dans de nombreux pays, vous avez une activité mondiale. Cette question de l'identité numérique est-elle abordée de la même façon partout en Europe ? Une comparaison avec l'Estonie n'est peut-être pas pertinente, car les niveaux de maturité sur l'identité numérique, les tailles de populations, les administrations, les histoires ne sont pas les mêmes. Mais parmi les pays qui nous ressemblent le plus, le retard pris par la France générera-t-il un retard supplémentaire ? Si nous sommes en train de rattraper le retard pris depuis quelques années, mais qu'eux ont avancé sur l'identité numérique, avons-nous besoin de faire un saut qualitatif dans ce que nous devons atteindre dans les quatre cents prochains jours ?

M. Bruno Bernard. Les quatre cents jours sont peut-être un peu ambitieux.

M. Philippe Latombe, rapporteur. Ce n'est pas mon calendrier.

M. Bruno Bernard. Il faut essayer de combler le retard d'il y a trois ans et atteindre un système à parité avec celui de nos voisins allemands et britanniques, toujours dans l'idée d'élaborer une identité numérique à l'échelle européenne, qui est le grand enjeu en la matière. Les processus de décision à cette échelle peuvent réserver des surprises et ne pas être optimaux, mais nous pouvons espérer que la présidence française de l'Union européenne qui s'annonce soit un accélérateur en Europe et en France sur nombre de ces sujets, dont l'identité numérique.

M. Philippe Latombe, rapporteur. Quand on parle d'identité numérique, on parle d'usages. Vous avez souligné tout à l'heure l'importance de l'éducation des collégiens, pour qu'ils ne soient pas uniquement des consommateurs, mais sachent comment le numérique fonctionne. Comment voyez-vous les usages du numérique dans les années à venir ? Quels sont les domaines dans lesquels la France et l'Europe doivent investir maintenant pour être à la pointe de ce qui se passera dans quelques années ?

En matière de *cloud*, par exemple, on nous a expliqué que nous ne serions jamais au niveau des géants actuels. Nous mettrons beaucoup de temps à les rejoindre, et cela nécessitera beaucoup d'efforts. On nous a dit à l'inverse que nous étions très en avance sur de nombreux sujets, dont l'Intelligence artificielle des objets, par exemple. Identifiez-vous des domaines sur lesquels les Européens devraient davantage capitaliser pour rester à la pointe ?

M. Laurent Degré. Dans le domaine de l'Intelligence artificielle et du quantique, nous avons des choses à faire et à dire. Le quantique révolutionnera les capacités de calcul et ouvrira des cas d'usage et des possibilités jamais connus. Il ne faut pas rater ce virage. Dans le domaine de l'Intelligence artificielle, nous avons de très bons acteurs.

En matière de cybersécurité, nous avons des champions français en Europe. Faisons encore plus d'investissements, aidons-les dans cet écosystème, dont nous faisons partie. Capitalisons sur ces atouts : nous ne sommes pas en retard dans le domaine de la cybersécurité, bien évidemment.

Il faut également travailler sur plusieurs technologies – la 6G, le *edge computing*, visant à ramener la capacité de calcul au plus près de l'utilisateur, l'Internet des objets.

M. Bruno Bernard. J'ajoute, si vous le permettez, la technologie *open RAM*, qui est la virtualisation des accès radio. Ce n'est pas une technologie tout à fait mature, mais Cisco est par exemple partenaire de Rakuten au Japon pour déployer un réseau téléphonique virtualisé. Il s'agit de l'une des grandes révolutions à venir dans le domaine des télécommunications. Les opérateurs européens, dont Orange, se sont engagés sur le sujet. Les opérateurs américains le sont déjà, et nous pensons que cela peut faire partie du futur des télécommunications en France. Cela impliquera une réflexion sur le *cloud* et la nécessité de réaliser des investissements lourds. Si votre réseau téléphonique fonctionne demain de façon complètement virtualisée, il faudra le localiser quelque part, ce qui pose la question du contrôle de la donnée, des infrastructures.

À mon sens, ce qui permettrait de grandir à l'échelle européenne et d'avoir enfin des acteurs mondiaux serait de disposer d'un véritable marché unifié, où l'on puisse à la fois lever des capitaux, mais aussi se développer en partenariat les uns avec les autres, en s'appuyant sur des acteurs de confiance, dont Cisco ou d'autres, pour grandir tous ensemble. L'environnement est aujourd'hui encore, un peu, voire très, morcelé, ce qui freine l'émergence de ces champions européens.

M. Philippe Latombe, rapporteur. Nous voyons que l'innovation des GAFAM est permise par des succès commerciaux forts qui leur permettent de dégager des moyens en R&D, qui est réalisée soit en interne, soit par des acquisitions. Comment fonctionne Cisco avec l'environnement des *start-up* ? Collaborez-vous avec elles ? En incubez-vous certaines, pour les absorber ensuite ? Les laissez-vous vivre, en les plaçant sous votre aile pour en faire des avantages commerciaux dans vos offres ? Comment fonctionnez-vous avec cet écosystème ?

M. Laurent Degré. Il n'existe pas de modèle unique, mais plusieurs options. En matière de R&D, Cisco ne se limite pas aux États-Unis, car l'intelligence n'est pas disponible en un seul endroit : elle est distribuée partout. Par ailleurs, l'expertise est difficile à trouver, car il s'agit d'un marché en constante innovation. Nous comptons plus d'une centaine d'ingénieurs en R&D en France. Cisco compte au total 26 000 ingénieurs dans le monde.

Notre équipe française de R&D travaille constamment dans des modes sinon d'incubation, du moins de codéveloppement avec des *start-up*, qui viennent nous présenter des idées et ont besoin de support, ou vers lesquelles nous nous tournons. Nos équipes ont pour mission de mener des activités de R&D au sens strict, mais également de réaliser une veille technologique du marché, d'accompagner l'écosystème. Parfois, au lieu de développer en interne, nous procédons à une acquisition – mais ce n'est pas systématique. Cybervision est par exemple issu de la *start-up* villeurbannaise Sentryo, avec laquelle nous travaillions en codéveloppement. Nous les avons accompagnés dans leur croissance. Il y avait à un moment donné un besoin de capital. Cisco a fait le choix d'en faire l'acquisition. Cybervision est devenu un acteur mondial de la cybersécurité dans le monde industriel, présent partout en Europe et dans le monde.

Nous ne poursuivons pas une stratégie unique : les décisions sont prises *ad hoc* en fonction de la course à l'innovation et des meilleures opportunités. Certaines choses peuvent être faites en interne, d'autres sont cherchées ailleurs. Il n'y a pas de schéma tout tracé.

M. Philippe Latombe, rapporteur. Nous avons ce matin auditionné le responsable de la cybersécurité d'Orange, qui nous expliquait que certaines entreprises françaises étaient achetées vingt-cinq fois la valeur de leur EBITDA, et qu'il était impossible de rivaliser avec

les entreprises américaines sur ce plan. Partagez-vous le sentiment d'une survalorisation ? Pourquoi ces entreprises sont-elles valorisées à ce point ?

M. Laurent Degré. Si ces sociétés sont achetées à ces prix, cela signifie qu'il existe de la compétence et de l'expertise en France. II s'agit donc d'une bonne nouvelle. Par ailleurs, ce n'est pas de la survalorisation, mais une valorisation de la compétence qui a un prix sur ce marché. La question se pose ensuite de savoir si nous avons la capacité de le faire, au niveau français ou européen, mais c'est une autre discussion. Il n'y a pas de survalorisation de ces sociétés, mais une simple valorisation de leur compétence.

M. Philippe Latombe, rapporteur. Voyez-vous un sujet que nous n'aurions pas abordé et que vous voudriez évoquer ?

M. Laurent Degré. Non. J'espère que nous vous avons apporté quelques éléments de réflexion. Nous restons à votre entière disposition. Il y a bien d'autres choses à couvrir, mais je n'ai rien à ajouter pour ma part.

M. Bruno Bernard. Nous nous tenons à votre disposition pour tout suivi ou complément d'information dont vous auriez besoin. De manière générale, Cisco a toujours la capacité de fournir une certaine expertise sur ces sujets. Nous sommes ravis de la partager.

La séance est levée à 14 heures.

Membres présents ou excusés

Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne »

Réunion du mardi 13 avril à treize heures

Présents. – Mme Danièle Hérin, MM. Philippe Latombe, Jean-Luc Warsmann