ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

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

Jeudi
11 février 2021
Séance de 11 heures

Compte rendu n° 27

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Jean-Luc Warsmann, *président, puis de M. Philippe Latombe, rapporteur*

ASSEMBLÉE NATIONALE

Audition commune, ouverte à la presse, de M. Jean-Noël de Galzain, président d'HEXATRUST, M. Stéphane Volant, président du Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE), et de Mme Florence G'Sell, professeure de droit à l'université de Lorraine, membre du Club des juristes

La séance est ouverte à 11 h 05.

Présidence de M. Jean-Luc Warsmann, président, puis de M. Philippe Latombe, rapporteur.

M. le président Jean-Luc Warsmann. Nous recevons aujourd'hui les représentants de HEXATRUST et du Club des Directeurs de Sécurité et de Sûreté des Entreprises (CDSE), ainsi que Mme le Pr Florence G'Sell, professeur de droit à l'université de Lorraine, qui est également contributrice régulière au sein du Club des Juristes.

L'audition de ce jour prend appui sur le manifeste intitulé « Cinq vœux pour une autonomie stratégique européenne » du mois de septembre 2020. Cette réflexion sur les enjeux et les conditions d'une souveraineté numérique, intéresse directement nos travaux. C'est la raison pour laquelle nous souhaitions échanger avec ces auteurs et ces contributeurs.

M. Philippe Latombe, rapporteur. J'aimerais tout d'abord que vous nous présentiez le contenu de votre manifeste, « Pour une autonomie stratégique européenne » et ses différents axes. Je pense notamment au soutien des PME françaises de confiance *via* l'instauration d'une proportion d'achats fléchés, et au soutien des investissements des entreprises dans les équipements numériques, qui ont déjà fait l'objet de plusieurs échanges au cours de nos travaux.

Ensuite, j'aimerais connaître votre point de vue sur le *cloud* et sa sécurisation. C'est l'objet même de l'existence du groupement HEXATRUST. Dressant le constat d'une hausse de la dépendance des entreprises à leur fournisseur de service *cloud*, le groupement promeut le recours à des prestataires de confiance et a récemment développé un label, le SecNumCloud, pour orienter les acheteurs. Ce label a dernièrement été obtenu par Outscale et OVHcloud. Selon vous, comment les pouvoirs publics peuvent-ils encourager davantage la diffusion d'une véritable culture de la cybersécurité chez les acteurs à la fois publics et privés ? Cela nous permettra d'échanger sur vos propositions concernant le sujet Cyber. Le CDSE pourra également nous dire un mot sur la perception des entreprises et leur adaptation à ces risques croissants.

Enfin, je voudrais revenir sur les différentes initiatives européennes touchant directement ces questions. Je souhaiterais vous interroger sur votre perception des différents projets en cours. Je pense notamment aux directives DSA *(Digital Services Act)* et DMA *(Digital Market Act)*. Je souhaite aussi vous entendre, d'une part, sur le *Data Governance Act*, et, d'autre part, sur la stratégie de cybersécurité présentée par la Commission européenne en fin d'année dernière. Ces projets vous paraissent-ils adaptés aux défis qui s'annoncent pour les prochaines années ?

M. Stéphane Volant, président du Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE). Je trouve intéressant de partir du besoin du client et de l'utilisateur. Ces derniers sont souvent oubliés sur ce sujet, sur lequel on nous vend des avions renifleurs et des éléphants blancs, ce qui n'est pas toujours très satisfaisant.

M. Jean-Noël de Galzain. Nous sommes d'accord.

M. Stéphane Volant. M. Jean-Noël de Galzain sourit, mais il voit bien, au sein de la filière des industries de sécurité où nous siégeons tous les deux, qu'il s'agit de notre obsession.

N'y voyez rien d'autre qu'une taquinerie, mais je vous invite à noter que nous échangeons sur Zoom. Même à l'Assemblée nationale, nous utilisons une application qui n'est pas entièrement française ni souveraine. Je vous rassure, vous n'êtes pas les seuls.

M. Philippe Latombe, rapporteur. Nous allons implémenter Tixeo dans les jours qui viennent, à la suite de remontées indiquant que Zoom n'était pas idéal.

M. Stéphane Volant. Je ne me plains pas. Nous avons juste mis en copie de nos échanges New York et Washington, mais nous ne traiterons pas de secrets d'État.

M. Philippe Latombe, rapporteur. Vous oubliez Pékin.

M. Stéphane Volant. Sachant que même les ministres de la Défense européens en Conseil de Défense ont des intrus dans leurs applications, nous pouvons imaginer qu'il reste un bout de chemin à faire. Il est formidable que vous implémentiez Tixeo.

Comme vous l'aurez noté pendant la période de confinement, en tant que père de famille ou en tant qu'utilisateur particulier, il n'existe aucune application française ni européenne capable d'offrir en masse, aux Français, de quoi échanger gratuitement et de manière simple sur les réseaux. Les applications existent – Tixeo en est une –, mais elles sont rares. Certaines sont payantes et surtout extrêmement malcommodes. Le confinement a montré que l'outil domestique n'existait pas.

Je travaillais encore récemment dans l'une des plus grandes entreprises nationales. La plupart des entreprises n'utilisent pas de solution française ni de solution européenne. Le marché des solutions françaises ou européennes des entreprises représenterait 10 % à 15 % des entreprises à l'heure actuelle. La raison n'est pas que les entreprises ne sont pas patriotes, surtout lorsqu'il s'agit d'entreprises publiques ou de défense. Ce n'est pas non plus parce qu'elles refusent de travailler avec des solutions françaises. Il y a deux raisons possibles : soit les solutions françaises sont inaccessibles et non compétitives, soit elles n'offrent pas les mêmes fonctionnalités ni la même ergonomie que les solutions internationales.

Je parle des entreprises françaises, mais je pourrais parler de l'État et des collectivités territoriales, qui se sont fait rappeler à l'ordre par la Commission nationale de l'informatique et des libertés (CNIL) encore récemment. La CNIL leur reprochait de mettre les données de santé des Français sur des solutions et des *clouds* qui n'étaient pas nationaux.

On nous parle de Campus Numérique à grands frais à La Défense. Je note que beaucoup de mètres carrés, d'inox et de verre lui sont consacrés, mais je ne sais pas si, à ce prix au mètre carré, nous verrons beaucoup de monde y prendre part.

On nous parle de GAIA-X, avec plein de GAFAM *inside*. En effet, à l'intérieur de GAIA-X, nous trouvons déjà des briques de Microsoft. C'est à croire que l'objet n'est déjà pas souverain, mais nous attendons de voir.

On nous parle d'un grand plan quantique national. En tant qu'utilisateur, je me réjouissais de ce plan, car je pensais que nous étions précurseurs sur le quantique, qui ne fait pas beaucoup parler de lui. En m'intéressant ce matin aux statistiques, j'ai découvert que la

Chine avait déposé l'année dernière 1 157 brevets en matière de quantique, que les USA en avaient déposé 363, la Grande-Bretagne 29, l'Allemagne 23 et la France 9. C'est dire notre retard, y compris sur ce sujet.

On nous parle de millions là où il faudrait des milliards.

On nous parle de demain, là où il faudrait parler d'aujourd'hui, voire d'hier.

Et on nous dit qu'Orange et Atos sont des chantres de la souveraineté, alors qu'ils ont des partenariats stratégiques avec Microsoft et communiquent à grands frais pour s'en vanter.

Bref, si je m'adresse à vous en tant qu'utilisateur, je pense qu'il va falloir un jour nous dire la vérité. Il va falloir cesser d'envisager de ne passer que par la contrainte pour que les particuliers comme les entreprises utilisent des solutions qui ne fonctionneraient pas sans cette contrainte. Les grandes entreprises, qui sont parfois gorgées d'argent public et de subventions, n'ont pas montré, ces dernières années, toute la force qu'elles auraient pu posséder. Nous attendons qu'elles laissent un peu la place aux PME et aux PMI, ainsi qu'aux start-up. C'est probablement chez ces dernières que nous trouverons le Mark Zuckerberg français. M. Jean-Noël de Galzain ne ressemble pas à Mark Zuckerberg, mais il en est un. Il est à la tête d'une association qui regroupe des start-up et de talentueux personnages. Il convient de nous poser les bonnes questions d'urgence et d'y apporter les bonnes réponses.

Les personnes qui se trouvent autour de la table sont capables de vous énoncer les critères de souveraineté à retenir. C'est la première chose à faire. Quels seront les critères qui permettront d'estampiller une solution « souveraine » et comment les rendre visibles auprès du grand public, comme des industriels ? Comment imposer ces critères dans les appels d'offres ? J'ai connu auparavant de grandes entreprises qui n'avaient pas d'autre choix que de passer par des solutions étrangères, parce que celles-ci étaient moins chères et plus performantes. Si l'on imagine que les solutions françaises de demain se montreront aussi performantes que les solutions étrangères, comment les imposer dans les appels d'offres ?

Vous noterez qu'il existe un organisme pour les personnes radicalisées dans les entreprises, le SNEAS (Service national des enquêtes administratives de sécurité). Quand vous embauchez quelqu'un, ou que vous faites la promotion d'emplois sensibles auprès de personnes au profil ou au comportement curieux, vous avez la possibilité d'interroger ce service, qui vous donne un *go* ou un *no go*. Il vous permet d'avancer officiellement les raisons pour lesquelles vous n'avez pas retenu une candidature ou accordé une promotion, y compris devant les Prud'hommes. Il serait judicieux, pour les produits numériques, de se doter d'un service analogue permettant de ne pas retenir, en appel d'offres, des solutions un peu plus concurrentielles que les françaises.

Comment surveiller ces critères de souveraineté sur la durée ? Aujourd'hui, de formidables petites sociétés sont souveraines pendant deux ans. Et puis, un grand État étranger s'aperçoit qu'il faut absolument entrer dans leur capital et elles ne le sont plus. Je l'ai vécu pendant le confinement. Le ministère de l'Intérieur m'a demandé d'utiliser une solution ; quelques semaines plus tard, le Secrétariat général de la défense et de la Sécurité nationale (SGDSN) m'a annoncé que le capital avait changé et qu'il ne fallait plus l'utiliser.

Dans la plateforme que nous partageons avec HEXATRUST et le Club des Juristes, nous avons émis un grand nombre de propositions.

Tout d'abord, il faut définitivement soutenir la R&D, non seulement celle des grands, mais aussi celle des PME et celle des start-up. Il nous faut également écouter les utilisateurs, qui ne veulent pas qu'on les contraigne à prendre des solutions souveraines exorbitantes et malcommodes, au motif qu'elles sont souveraines. Le coût de la souveraineté représente un supplément de 10 % à 15 %. C'est une assurance, mais nous ne pourrons pas aller au-delà. Encore faut-il que nous nous saisissions de la question des critères de la souveraineté et que les entreprises soient assurées, pour 15 % de plus, de ne pas se faire piller leurs données et de pouvoir parler à leurs clients en toute tranquillité.

Nous disposons aujourd'hui d'un outil formidable, qui est la filière des industries de sécurité – comme vous le savez, l'industrie française est organisée en filières. À l'intérieur de cette filière, se trouvent des acteurs de taille importante, moyenne et petite, ainsi que les utilisateurs. C'est une grande première. Donnons sa chance à cette filière. Si nous respectons les équilibres grands/moyens/petits/utilisateurs, nous devrions obtenir des solutions pratiques et souveraines nationales.

Enfin, l'année 2021 sera décisive. Beaucoup de choses ont été dites depuis des décennies en matière de souveraineté numérique. Nous arrivons au bout d'un cycle. Si les grands projets menés avec le Campus de la Cybersécurité et avec GAIA-X n'aboutissent pas rapidement, les utilisateurs n'y croiront plus. La France et l'Europe devront alors peut-être faire le deuil de cette souveraineté-là et passer à autre chose, en admettant qu'elles n'ont pas réussi, avec leurs moyens propres, à s'adresser à ce marché crucial pour nos industries et nos familles – lorsque nous emmenons l'ordinateur chez nous pour travailler avec un logiciel, le travail et la famille sont interconnectés.

Je vous demande pardon pour mon impertinence, mais l'utilisateur est lassé de se faire « raconter des fariboles ». On nous promet la souveraineté pour demain. On nous promet des solutions françaises pour demain. Cela fait des années que c'est pour demain. Quand nous entendons dire que ces solutions, qui ne sont pas retenues parce qu'elles ne sont pas au niveau, devraient nous être imposées par la loi, nous faisons des bonds, chez les industriels comme les particuliers.

M. Jean-Noël de Galzain, président d'HEXATRUST. Je suis ravi d'être auditionné avec M. Stéphane Volant et avec le CDSE. En effet, nous considérons aussi que, pour rebâtir cette souveraineté et changer notre modèle, qui appauvrit visiblement cette souveraineté, il convient de commencer par associer les utilisateurs, qui sont les bénéficiaires, aux innovateurs, qui inventent des produits, des services et des modèles nouveaux. Telle est la thèse qui nous a conduits à rédiger ce manifeste. Nous assistons à une répétition de l'histoire, qui consiste à réutiliser en permanence des organismes et des organisations déjà existantes et à utiliser un modèle arrêté entre les grandes organisations et l'État. Ce modèle est à bout de souffle. Nous proposons un modèle de reconstruction différent, dans un domaine qui nous a échappé.

Je suis à la tête d'une organisation, HEXATRUST, qui regroupe un certain nombre d'organisations, telles que des start-up, des PME et des ETI spécialisées dans la cybersécurité, le *cloud* de confiance et la mise en œuvre d'un environnement numérique de confiance. C'est sur cette base que j'avais lancé le forum international de la cybercriminalité à Lille, il y a deux ans.

En matière de numérique, nous sommes aujourd'hui ballottés entre deux mondes, pour reprendre la formule d'Eric Schmidt, le patron de Google à l'époque. Nous sommes ballottés

entre un monde numérique chinois organisé au bénéfice des organisations gouvernementales et du système chinois, et le reste du monde emmené par les Américains. Une opportunité historique se présente à nous, celle de créer le numérique de confiance, c'est-à-dire un environnement numérique éthique, protecteur des données personnelles, et garantissant les critères de liberté, d'autonomie et donc de souveraineté.

Ce numérique doit s'imposer dans un environnement qui n'est pas le nôtre, puisque nous utilisons un numérique essentiellement américain, en tant qu'alliés des États-Unis. Les *clouds* sont presque tous américains et les moteurs de recherche Internet sont tous américains. Cet environnement est certes hostile au départ, mais, à terme, le numérique de confiance, qui sera un numérique RGPD respectant toutes les réglementations européennes et nos règles démocratiques, intéressera le monde entier et comptera beaucoup plus d'utilisateurs que les GAFAM d'aujourd'hui, si nous sommes capables de tenir sur ce registre et de le mettre en œuvre.

Le deuxième aspect s'appuie sur un constat. Certes, nous avons perdu la bataille des GAFAM. Le monde de la technologie de l'information (IT) compte aujourd'hui un grand nombre de start-up et d'entreprises ayant quantité d'utilisateurs présents sur les réseaux sociaux. Nous avons des difficultés à maîtriser ces derniers, qui bousculent nos règles et influent même sur nos processus démocratiques. Je pense que cette bataille n'est pas le combat du moment. La bataille que nous devons mener est celle de l'industrie 4.0, c'est-à-dire de l'industrie du futur, mais aussi celle de la modernisation de nos gouvernements, de nos hôpitaux et de nos systèmes de santé – demain, la santé sera numérique. La bataille concerne aussi la modernisation de nos villes avec l'émergence des *Smart Cities* et des *Smart territoires*, et tout ce qui permettra l'accès pour tous au numérique et la mise en place de l'Internet des objets.

Pour tous ces aspects, qui n'en sont qu'à leurs prémices, nous avons besoin de plateformes et de systèmes numériques qui soient, à la fois, fiables, robustes et dans lesquels la protection des données est essentielle. Il s'agit de l'actif du futur et de ce qui va venir alimenter les algorithmes d'intelligence artificielle qui nous permettront d'augmenter le bonheur et l'utilité du numérique dans nos vies. La bataille se situe sur ce terrain.

Tout notre enjeu, en tant que professionnels de la cybersécurité, professionnels de l'Internet de confiance, mais aussi PME, start-up ou ETI françaises, luxembourgeoises ou allemandes, est de faire en sorte que ce numérique voie le jour.

Pour ce faire, il est essentiel de mettre en place une stratégie d'exécution. En effet, l'une des raisons essentielles pour lesquelles nous sommes perdants dans la bataille numérique 1.0 (ou numérique des pionniers) est que nous n'y avons pas cru. Nous n'avons pas vu venir le changement. Nous avons considéré l'IT et le numérique comme relevant des start-up, de l'innovation, de préoccupations lointaines et annexes. Ce domaine est en réalité devenu une industrie dans laquelle des pays, tels que les États-Unis et la Chine, se sont mobilisés et ont investi massivement, en utilisant leurs organismes publics et leurs ministères de la Défense. Ces pays ont également recouru à une forme de protectionnisme et de soutien auprès de leurs start-up en leur apportant des financements et des commandes, dès le départ, afin de les massifier et d'en faire des géants mondiaux. Ces financements ont été relayés par une bourse alimentée par des fonds de pension. Ces derniers ont les moyens de financer les phases ultérieures de croissance de ces start-up et de ces PME.

Il est ainsi essentiel de massifier et de fluidifier le marché européen, afin que nos entreprises, nos PME et nos start-up puissent avoir accès plus rapidement au marché des utilisateurs. Sur tous les marchés et les domaines sensibles, nous devons prêter une attention particulière aux solutions dans lesquelles nous hébergeons des données, des systèmes et des applications, ainsi qu'aux solutions de contrôle et de protection que nous mettons en place. Nous devons vérifier que les solutions utilisées dans ces domaines sont certifiées par les organismes européens.

Dans notre manifeste, nous avons énoncé cinq grandes mesures.

La première est de mener un plan d'équipement massif dans un certain nombre de domaines, qui ont été oubliés dans la transformation numérique. La pandémie que nous traversons met en lumière le fossé qui existe entre les privilégiés du numérique et un certain nombre de PME, ETI, artisans, professions libérales, commerçants, mais aussi tout un nombre d'organisations publiques de santé et de collectivités locales, qui ne sont pas équipés comme il se doit. Nous pensons qu'il faut mettre en place des plans d'équipement, voire utiliser des fonds structurels pour permettre à des groupements d'utilisateurs de bénéficier d'une aide à l'équipement de produits numériques, de cybersécurité et d'hébergement.

La deuxième mesure consiste à flécher au maximum tout argent public dépensé dans les relances, dans les plans stratégiques européens ou dans les plans d'équipement, afin que cet argent revienne en priorité à nos entreprises et à nos industries. Il doit permettre aux PME, start-up et ETI de se transformer en entreprises de taille intermédiaire et en futures grandes entreprises, en industrie de la cybersécurité, du *cloud* et du numérique. Nous pensons qu'il faut flécher une grosse partie de ces investissements vers les PME, comme cela a été fait après la Seconde Guerre Mondiale aux États-Unis, avec le *Small Business Act*. Il nous faudrait un *Buy European Act*. Nous allons travailler avec l'association France Digitale pour avancer sur ces sujets. C'est aujourd'hui qu'il faut le faire, compte tenu de tout l'investissement prévu dans la modernisation et la transformation digitale.

Le troisième aspect est de construire une Europe de la Cybersécurité. Nous avons besoin d'aborder le sujet à l'échelle européenne. Il est plus que jamais intéressant de construire un territoire numérique de confiance capable de fédérer l'ensemble des Européens. Il sera plus difficile de fédérer les Européens dans la vraie vie, parce que nos pays ont tous une souveraineté très importante. Mais en matière de numérique, il n'existe pas de souveraineté dans nos pays. L'Europe n'a pas d'existence propre dans le monde du numérique. C'est le moment ou jamais de réunir les Européens sur un sujet essentiel, qui est le numérique de confiance.

Nous pensons qu'il est urgent d'avoir une stratégie au niveau européen, de nous doter d'un ministère de l'industrie européen. Il s'agit d'investir massivement dans des solutions de financement en Europe pour permettre à nos entreprises et à nos industries de se développer. Il s'agit aussi d'encourager GAIA-X à faire émerger des start-up, des innovateurs, des PME et des projets de recherche, qui permettront de faire jaillir autre chose que des GAFAM, c'est-à-dire de nouvelles organisations basées sur ce numérique de confiance.

La quatrième mesure est de financer les ETI, les PME et les start-up de croissance. Cet aspect est essentiel. Arrêtons de croire que nous allons changer le monde en investissant de l'argent dans les grandes entreprises. Si nous réservons de l'argent aux PME, start-up et ETI, et si leurs propositions de valeur séduit les utilisateurs, alors nous parviendrons à attirer les grands intégrateurs, les grands financeurs et les grandes banques. Le cercle vertueux

fonctionnera, puisque nous créerons de nouveaux besoins et de nouveaux marchés. À cette création de valeur, succède un ruissellement. Nous avons pris ce ruissellement à l'envers. Il doit commencer par les petits, qui seront ensuite aidés par les grands pour passer à l'échelle supérieure. Le fait de financer les PME et les ETI implique de mettre des moyens à la Banque européenne d'investissement, afin que nous y ayons accès.

S'agissant d'une PME comme Wallix, la société que je dirige, la Banque européenne d'investissement propose de l'aide, ce qui est un point positif. Mais quand nous demandons cette aide, nous nous trouvons avec des taux de prêts allant de 13 % à 17 % par an. C'est prohibitif. Ainsi, les solutions de financement existent, mais elles sont inaccessibles aux PME et aux ETI. Il faut par conséquent changer les mentalités. Aujourd'hui, une entreprise comme Thales peut emprunter à 1 % ou à 3 %. Nous devons être en mesure de le faire également. Il faut de grands fonds d'investissement permettant aux investisseurs qui sortent au fur et à mesure de nos entreprises de ne pas avoir à revendre systématiquement l'entreprise à un fonds américain ou à un grand industriel américain, qui pourra, quant à lui, payer la juste valeur pour les entrepreneurs.

À noter que la revente de la société Alcide, une pépite de la cybersécurité, a été annoncée hier pour 98 millions de dollars. Nous ne pouvons pas acheter ces entreprises en Europe si nous n'avons pas les solutions de financement pour le faire.

Enfin, le cinquième aspect concerne l'assurance. Les réglementations ont permis de faire émerger le RGPD. Nous sommes en train de mettre en place NIS 2, qui viendra moderniser la directive NIS *(Network and Information Security)* pour l'étendre à d'autres entreprises. Le Règlement général sur la protection des données est structurant pour l'Europe et pour notre démocratie. Le problème est que beaucoup de gens ne sont pas en mesure de se défendre ou de mettre en application cette protection des données dans leur organisation. Par conséquent, il faut étendre la responsabilité civile à la cybersécurité et à la protection des données, afin que même les plus petites organisations, les entrepreneurs individuels et les TPE, puissent avoir accès à la protection des données et à la protection cyber.

Pr Florence G'Sell, professeure de droit à l'université de Lorraine. Sur la question de la souveraineté numérique, je souhaite partir d'un exemple tout récent. Il s'agit tout simplement du bras de fer qui se joue actuellement entre Twitter et le gouvernement indien.

Le gouvernement indien affronte aujourd'hui une forte contestation en raison d'une réforme agricole. Des mouvements de protestation se sont déroulés à New Delhi, où les paysans sont descendus dans la rue. Dans ce contexte, le gouvernement indien a demandé à Twitter de suspendre ou de bloquer des comptes de personnes appelant à la sédition. Twitter a obtempéré jusqu'à un certain point, tout en refusant de suspendre les comptes de certaines personnes considérées comme des journalistes, des activistes ou assumant des responsabilités politiques. Cela donne lieu à un bras de fer entre le gouvernement indien et Twitter. Ce dernier argue que ses conditions d'utilisation doivent être appliquées en l'état, et considère que sa démarche est conforme au droit indien. De son côté, le gouvernement souligne qu'il dispose de texte permettant de jeter en prison les représentants de Twitter présents sur le sol national s'ils ne respectent pas ses demandes et ses règles.

Cette affaire exprime bien la manière dont nous pouvons envisager la question de la souveraineté numérique, à travers l'idée d'un bras de fer entre les États et les plateformes. Même si des règles juridiques s'appliquent au monde virtuel et aux plateformes, celles-ci ont acquis une telle force de frappe et une telle indépendance qu'elles sont en mesure de faire ce

qu'elles veulent, de fonctionner en se référant d'abord à leurs conditions d'utilisation. Ces plateformes s'appuient aussi sur le fait qu'elles sont implantées aux États-Unis et qu'elles se conforment avant tout à la législation américaine.

Cela représente aujourd'hui une vraie difficulté, qui relève du cœur de ce que nous appelons la souveraineté. Dans notre République, la souveraineté est celle du peuple, mais nous l'exerçons au travers de nos représentants et elle est incarnée par l'État. Cette affirmation de l'autorité de l'État pose un problème dans le monde virtuel, *a fortiori* face à des plateformes de cette taille et donc de cette puissance.

Le volet de la souveraineté comprend bien évidemment d'autres aspects. Qui dit souveraineté dit aussi indépendance, c'est-à-dire indépendance technologique. Nous avons pris conscience, à la faveur de la crise sanitaire, de notre dépendance à des technologies principalement américaines – nous sommes aujourd'hui sur Zoom et j'enseigne avec ces outils depuis presque un an maintenant. De fait, nous avons en permanence le sentiment de buter sur cette dépendance technologique pour un grand nombre de sujets, en particulier la question du stockage des données.

On nous dit que les grands fournisseurs, comme Amazon, Microsoft et Google, sont ceux qui présentent les meilleurs services au moindre coût. Ce volet, un peu moins juridique, de la souveraineté numérique englobe l'idée de la *data sovereignty*, ou souveraineté des data, dont nous parlons beaucoup dans la littérature académique. Est-ce une bonne ou une mauvaise chose, une bonne ou une mauvaise stratégie ?

Enfin, la souveraineté est aussi celle du peuple. Dans l'univers numérique, le peuple a son mot à dire. Parfois, nous utilisons ce terme pour dire que nous avons tous, en tant que citoyens, le droit de reprendre la main, de ne pas nous faire imposer par les plateformes des conditions d'utilisation, des algorithmes ou des collectes de nos données que nous ne souhaitons pas. Là encore, nous pourrions imaginer l'existence de nouveaux droits fondamentaux en ligne, qui refléteraient ceux dont nous disposons dans le monde réel.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur un sujet que vous avez abordé tous les trois : le *cloud*. Certaines entreprises publiques ou émanations de l'État ont fait le choix d'aller vers des *clouds* non souverains. Je pense au Health Data Hub (HDH), à BPIfrance, mais aussi, récemment, à Engie ou à la SNCF, qui a décidé de mettre toutes les données de ses gares connectées sur un *cloud* non souverain. Outre la simplicité d'utilisation des *clouds* et de l'ensemble des produits qui vont avec, ces entreprises affirment s'être assurées que les serveurs étaient bien localisés en France ou en Europe, que la clé de chiffrement leur appartenait exclusivement et qu'il n'y avait donc pas de souci. Qu'en pensez-vous après le séisme de *Schrems* II ? La question n'est pas seulement juridique. Est-ce que *Schrems* II n'entre pas en contradiction avec cette vision ? Est-il suffisant de tout chiffrer chez nous et de localiser les données sur des serveurs européens, voire en France ? Le label SecNumCloud ne devrait-il pas intégrer un volet souveraineté ? Aujourd'hui, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pose des conditions techniques, mais ne parle pas de souveraineté dans son label. Faut-il ajouter un volet de souveraineté comme critère dans le SecNumCloud ou bien faut-il créer un label en plus relatif à la souveraineté ?

M. Stéphane Volant. J'ai été confronté, et les adhérents du CDSE le sont encore, à ce genre de difficulté dans des appels d'offres. La vraie difficulté n'est pas de savoir si ceux qui décident de recourir à des solutions non souveraines sont des naïfs. Avant cela, il faut se

préoccuper des critères que la loi impose dans les appels d'offres. Quand vous êtes face à diverses solutions dont aucune ne vous est officiellement interdite, que vous trouvez une solution moins coûteuse et beaucoup plus performante que les autres, et que la plus coûteuse porte un drapeau national, vous n'allez pas pour autant retenir la solution souveraine. Tout d'abord, ce n'est pas votre intérêt. Ensuite, parce que certains règlements d'appel d'offres vous encouragent à vous tourner vers le moins-disant et non vers le mieux-disant.

C'est pour cette raison que l'ANSSI doit précisément lister les critères de souveraineté, afin qu'il soit possible, au moment de l'appel d'offres, de les appréhender comme tels avec un organisme d'État ou un organisme indépendant.

Le fait d'être souverain vous contraint à être raisonnablement plus cher que les autres. Toutefois, le « raisonnablement » est important. Vous ne pouvez pas, au motif que vous êtes souverain, présenter une offre 50 % ou 60 % plus chère que les autres. Cela doit aussi vous encourager à proposer les mêmes fonctionnalités et la même ergonomie que les solutions de vos concurrents. En effet, si pour un prix identique vous offrez deux fois moins de services et qu'il est trois fois plus difficile d'y accéder, cela ne fonctionnera pas.

Il convient d'aborder le prix de la souveraineté. Des études sont en cours sur ce sujet. Il faut que nous diffusions davantage l'idée que la souveraineté doit être vécue comme une assurance. Au moment où une personne paie sa police d'assurance, celle-ci paraît toujours très chère, mais le jour où les six étages du dessous sont inondés, la personne est très contente d'avoir payé la police d'assurance. En matière de numérique et de souveraineté, c'est la même chose.

Enfin, je pense qu'il faut disposer d'un outil qui permette, dans les appels d'offres, de contourner un certain nombre de règles imposant de prendre le moins-disant. Je faisais précédemment le parallèle avec le fameux SNEAS, qui permet de contourner le code du travail pour prendre en compte le caractère dangereux de la montée du radicalisme dans les entreprises, et d'avoir un organisme d'État qui s'oppose officiellement à l'embauche ou à la promotion de quelques personnels. La loi et le système sont encore imparfaits, mais c'est un bon début. Il faudrait disposer, au moment des appels d'offres, d'un papier de l'ANSSI ou d'un autre organisme avec la mention suivante : *« Vous ne pouvez pas retenir, au nom de la souveraineté nationale et donc de vos intérêts d'entreprise, cette solution-là. Nous vous l'écrivons et vous pouvez produire ce papier dans le cadre des commissions d'appel d'offres »*. En matière de montée de la radicalisation, nous pouvons en effet produire un papier du SNEAS, par exemple aux Prud'hommes. Un tel document sur la souveraineté nous serait d'une énorme utilité. Aujourd'hui, l'ANSSI fait un travail remarquable, mais nous appelle seulement en *off* pour nous demander d'éviter de choisir une solution. Non seulement ce n'est pas officiel, mais la solution à éviter est souvent moins chère, plus performante et plus facile d'accès. Il va falloir que nous fassions un effort.

Ce point de vue est celui de l'utilisateur. Il est peut-être « proche des pâquerettes », mais il représente la vraie vie d'une commission d'appel d'offres et d'un dirigeant d'entreprise. Celui-ci se soucie bien entendu des intérêts nationaux, mais il est également piloté par son compte d'exploitation et ne dispose pas des outils juridiques lui permettant de répondre à un certain nombre de vos interpellations.

M. Jean-Noël de Galzain. Il règne tout de même une grosse hypocrisie sur les questions de prix et de compétitivité. En effet, sans le niveau d'imposition existant en France pour les entreprises, notamment pour les PME, sans certaines contraintes en matière de

réglementations et d'obligations, sans le niveau administratif et l'ensemble des prestations sociales prises en compte dans le calcul d'un prix en France, alors nous sommes effectivement plus compétitifs. Les prix doivent être regardés à la lumière de ce qu'ils incluent. Nous ne pouvons pas continuer à admettre une telle distorsion de concurrence, avec des entreprises qui ne paient pas d'impôts, qui vendent sans TVA ou avec une TVA réduite, et qui ne respectent aucune des réglementations qui leur sont imposées, lorsqu'elles ont une entreprise basée en France. Évidemment, certains acteurs industriels globaux arrivent à utiliser ces mécanismes d'optimisation et échappent ainsi aux réglementations des États. Or les PME, start-up et ETI n'ont aucun moyen d'y échapper. Avez-vous envie d'un monde dans lequel règne l'individualisation des profits au détriment de la collectivité ? Je n'en suis pas certain. Je suis plutôt pour un numérique éthique et durable, dans lequel nous respectons les meilleurs aspects de notre modèle de société.

Concernant votre question même, je crois que nous sommes dans un état d'urgence. Les monopoles empêchent nos entreprises de se développer et de se battre à armes égales. Dans cette période de pandémie, où nous devons construire à toute vitesse un environnement numérique fiable, avec des systèmes numériques qui protègent les données et garantissent toutes ces règles, nous sommes dans un moment d'exception. Après l'urgence sanitaire, nous entrons dans une urgence numérique.

Dans ce climat d'urgence numérique, faut-il appliquer le principe de précaution ? Ou plutôt, pourquoi ne pas appliquer le principe de précaution au numérique ? Par conséquent, il convient de se demander si nous devons gagner 1 %, 2 % ou 5 % de fonctionnalités au détriment de toutes les règles de protection des données, de protection de la vie privée et de protection contre les risques liés à l'utilisation de ces données dans des intelligences artificielles qui ne seront pas les nôtres, qui ne respecteront pas nos us culturels, et qui utiliseront du temps de notre vie dans le futur.

Il est important d'introduire des critères de souveraineté dans nos achats. Nous sommes en effet dans une phase de reconstruction. Il est urgent de le faire, parce que c'est la condition *sine qua non* pour créer un marché européen digne de ce nom. Par ailleurs, en voyageant dans différents pays, avant la pandémie, je me suis rendu compte que certains d'entre eux pratiquaient, dans leurs achats, une primauté des solutions locales. En particulier, lorsque l'argent public est concerné, l'existence de contreparties est vérifiée en matière d'emploi local et de respect des productions locales. Il s'agit de s'assurer que les règles du pays en question sont respectées. Je l'ai vu dans différents territoires, notamment en Asie, en Russie et même aux États-Unis, où il existe une telle primauté sur certains marchés.

Ainsi, pour le *cloud* gouvernemental américain, des appels d'offres géants ont été lancés. Les acteurs reconnus ont été exclusivement les grands acteurs du *cloud* américain. Personne n'a cillé sur le sujet. Aujourd'hui, il faut être conscient de notre responsabilité et faire en sorte d'introduire plus de souveraineté dans nos achats.

Ensuite, les *clouds* sont capables d'être compétitifs, y compris quand il s'agit de *clouds* souverains. Pour bien connaître les personnes d'OVH, d'Outscale ou d'autres organisations de cette nature, je sais qu'elles sont capables d'apporter, dans des temps très courts, si l'investissement est présent, des solutions compétitives pour nos organisations. Il faut placer aujourd'hui la souveraineté dans les critères d'achat et dans des clauses administratives générales.

Pour étendre le sujet à la sphère privée, les notions de responsabilité numérique environnementale ou de responsabilité sociétale et environnementale nous incitent à utiliser un numérique soutenable, à moyen et à long terme, lorsque nous achetons des ressources numériques.

Pr Florence G'Sell. Je n'ai pas la compétence me permettant d'identifier les prestataires les plus compétitifs, les plus compétents ou offrant les meilleures garanties. En revanche, je souhaite signaler que depuis l'arrêt *Schrems*, des recommandations ont été faites. Elles proviennent notamment du Comité européen de la Protection des Données, qui, à la suite de l'invalidation du *Privacy Shield*, a fixé une feuille de route pour les questions du choix du prestataire, du traitement des données et de l'exportation éventuelle des données. Parmi les mesures complémentaires que nous pourrions être amenés à prendre, lorsque nous souhaitons transférer des données sur la base de clauses contractuelles types, nous trouvons le chiffrement et le fait de détenir les clés de chiffrement. Cela fait partie des éléments listés, à l'instar de la pseudonymisation, par le Comité européen, dans cette recommandation du mois de novembre.

Il convient effectivement d'intégrer ces recommandations dans les cahiers des charges et dans les choix que nous faisons. Quant à savoir s'il faut privilégier par principe des solutions souveraines, je n'ai pas de position de principe sur le sujet.

M. Philippe Latombe, rapporteur. Pour élargir le sujet du *cloud*, vous dites qu'il faudrait nous doter d'un *Buy European Act*, en parallèle du *Small Business Act* américain. Qu'est-ce qui permettrait aujourd'hui de le mettre en place ? Doit-on le faire au niveau européen, ou bien au niveau national, si l'Europe n'y parvient pas dans un premier temps ? Comment pouvons-nous nous affranchir d'un certain nombre de règles européennes, notamment sur les marchés publics, si nous n'atteignons pas cet objectif global ? Vu le nombre de pays européens et le processus de décision européen, comment procéder ?

M. Stéphane Volant. J'ai un point de désaccord avec mon collègue, M. Jean-Noël de Galzain. Si 10 % à 15 % seulement des entreprises françaises passent par des solutions souveraines, alors que les 85 % restants comptent des entreprises nationales et de défense, ce n'est probablement pas parce que leurs dirigeants n'ont aucune fibre patriotique ni parce qu'ils n'ont l'œil rivé sur leur compte d'exploitation. C'est probablement parce que le prix des solutions françaises est exorbitant, que leurs fonctionnalités ne sont pas encore au niveau et que leur ergonomie est difficile d'accès.

Je rejoins M. Jean-Noël de Galzain sur le fait qu'il faut faire un effort massif pour augmenter les performances des entreprises dans ces domaines. Mais peut-être faut-il également augmenter de manière massive le soutien aux PME, aux PMI et aux start-up qui, dans ce domaine, n'ont peut-être pas eu toutes les chances dont tous les grands industriels français ont bénéficié.

En tout cas, avant de passer par la contrainte, qui pourrait être une directive européenne transposée en droit français, il convient de s'assurer que nous disposons de solutions de qualité suffisante, et que ces lois ne nous feront pas faire un saut en arrière et perdre un avantage technologique que nous pourrions avoir avec une solution étrangère.

Je suis comme nous tous extrêmement soucieux de l'intérêt national et parfaitement conscient des atteintes à notre souveraineté, inhérentes à l'utilisation de ces solutions étrangères. Mais attention à ne pas nous bercer d'illusions. Si le client ne retient pas de

solution souveraine et nationale à 85 %, y compris quand il est public ou de défense, ce n'est pas parce qu'il est idiot ou antipatriotique, mais probablement parce qu'il n'y a pas sur étagère de solution concurrentielle dans ce domaine.

M. Jean-Noël de Galzain, sommes-nous en désaccord ?

M. Jean-Noël de Galzain. Il est vrai que nous avons un train de retard. Nous sommes très en retard parce que nous n'avons pas de virtualiseur et très peu de piles logicielles sur nos infrastructures. Nous ne sommes pas non plus présents sur les systèmes.

Dans le domaine du logiciel libre en revanche, nous avons l'opportunité de rattraper notre retard et de mettre en œuvre une pile technologique indépendante qui nous permettrait de retrouver de la souveraineté numérique, au sens technique du terme.

Vous avez évoqué le HDH : certes le HDH a, à court terme, choisi le meilleur d'un point de vue technologique, au détriment de certains critères de souveraineté, mais il a également décidé de mettre en œuvre des solutions de cybersécurité, afin de vérifier les flux et de travailler sur les accès, les identités et le chiffrement en utilisant des solutions souveraines et certifiées. Je peux en témoigner puisqu'il s'agit de l'un de nos clients.

Lorsque nous avons le choix entre différentes solutions, l'alliance entre des solutions numériques de cette nature et des solutions de contrôle et de cybersécurité, qui, elles, s'avèrent certifiées et souveraines, peut déjà permettre la mise en place d'une première solution temporaire. Mais encore faut-il s'autoriser ce balancement, car je connais des entreprises qui sont en phase d'externalisation complète de leurs activités, par exemple en Inde ou au Maroc, et dans le même temps, confient à ce même hébergeur leurs problématiques de cybersécurité. Il s'agit donc assurément d'entreprises qui, pour le coup, n'auront plus aucun contrôle sur leur souveraineté IT.

Je pense qu'il convient d'aborder la souveraineté dans les achats au niveau européen (*Buy European Act*) pour une question de taille de marché. En effet, les entreprises américaines sont leaders parce qu'elles sont bien aidées au départ, mais aussi parce qu'elles bénéficient d'un marché intérieur considérable. Nous-mêmes devons *a contrario* faire certifier nos produits dans plusieurs pays. Un travail est d'ailleurs en cours avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), visant à permettre une sorte de reconnaissance mutuelle des différentes certifications nationales en matière de sécurité, afin de faire de nos produits de cybersécurité des produits de confiance, recommandés dans le cadre des directives NIS, du RGPD et autres. Il est en effet essentiel que nous puissions obtenir soit des certifications au niveau européen, soit une reconnaissance mutuelle des certifications nationales. Pour démarrer, nous pourrions commencer par la France et l'Allemagne, puisque nous collaborons beaucoup dans ces domaines. Nous avons besoin d'une taille de marché qui permette à nos entreprises de grandir plus rapidement.

De plus, afin de donner l'exemple, je crois que nous ne devons pas hésiter à commencer au niveau national, comme nous l'avons fait pour la taxe GAFAM. Cet effort de reconstruction doit être initié dès à présent : en effet, au sortir de la crise consécutive à la crise sanitaire, des milliers de milliards d'euros seront investis dans de nouvelles infrastructures, dans la modernisation et dans la transformation digitale, de la sphère privée comme de la sphère publique. Ces investissements concerneront tout le monde, c'est pourquoi il faut, selon moi, réserver une part de l'investissement public à l'émergence d'une industrie européenne, qui crée de l'emploi local, favorise la création de centres de données locaux et nous permet de

reprendre la main sur notre destin, en lieu et place du sempiternel argument juridique utilisé pour tenter de surnager dans un monde numérique que nous ne contrôlons pas. Si nous n'avons pas les clefs du numérique, nous continuerons à courir après le numérique de quelqu'un d'autre, qui, au bout d'un moment, utilisera l'intelligence artificielle en tant que service après-vente pour les questions juridiques, tout en continuant à investir dans son avance technologique, face à laquelle nous avons pourtant les moyens d'exister. Dans le domaine de la santé, comme dans les télécoms, l'IT, le numérique ou encore la cybersécurité, nos chercheurs, nos start-up et nos entrepreneurs travaillent pour des entreprises américaines, notamment. Nous disposons donc de tout le potentiel nécessaire.

Il ne manque plus qu'une volonté politique de mise en œuvre, au niveau européen, qui ne devra pas nous empêcher d'être offensifs, comme nous l'avons été à propos de la taxe GAFAM, en prenant des initiatives d'abord en France.

M. Philippe Latombe, rapporteur. Je souhaite revenir quelques instants sur votre propos selon lequel il peut exister des solutions qui, au départ, utilisent par exemple des *clouds* américains, dont nous n'avons pas pu nous passer, même pour notre solution hybride, puisque nous n'avions pas l'équivalent au niveau européen. Vous avez en effet expliqué que ces derniers peuvent utiliser des solutions de chiffrement souveraines.

Or il nous a été dit, lors des précédentes auditions, qu'il existait un risque assez fort d'addiction à ces produits : comme pour n'importe quelle drogue, les essayer reviendrait à se laisser « embarquer », d'abord parce qu'elles sont plus simples, d'où des développements internes facilités qu'il ne rimerait à rien de modifier par la suite. En outre, pour ceux qui doivent les abandonner, comme tel est le cas du HDH, la réversibilité ne s'avère pas simple, pour des raisons technologiques certes, mais surtout pour des raisons de coûts, car si une bande passante entrante ne revient pas très cher, une bande passante sortante s'avère bien plus coûteuse.

Ce constat relativise-t-il votre précédent propos ? S'agit-il d'une vraie crainte ? Le droit doit-il, en la matière, être moteur ? Devons-nous modifier les règles de concurrence sur cette pratique qui consiste à facturer plus cher les bandes passantes sortantes que les bandes passantes entrantes, en raison de laquelle les entreprises demeurent captives ?

M. Jean-Noël de Galzain. Le projet GAIA-X emporte un travail essentiel sur la réversibilité entre les différents *clouds*. Un chantier du projet de cybersécurité de la filière des industries de sécurité porte également sur la notion de réversibilité dans le *cloud*, dans la mesure où, pour l'essentiel, nous sommes actuellement obligés d'héberger des données et applications sur des *clouds* qui ne sont pas les nôtres, mais dont nous espérons pouvoir sortir.

Nous travaillons donc sur la réversibilité pour des raisons de coûts, mais aussi parce que nous rêvons de pouvoir bénéficier de *clouds* plus souverains. Il existe effectivement un problème de réversibilité bien connu, c'est pourquoi d'ailleurs la notion d'écosystème revêt également une grande importance, tout comme l'interopérabilité entre les solutions et le fait de donner de la visibilité aux projets de cette nature.

Pour ma part, j'apprécie les travaux du HDH qui mène de grands projets étendards : nous avons ainsi proposé, dans le cadre du comité stratégique de filière, de mettre à niveau la cybersécurité de tous les établissements hospitaliers de France (CH et CHU), parce qu'il s'agit de projets dans lesquels toute l'industrie entend intervenir, au côté de l'État, pour faire exister les solutions et infrastructures et les mettre en pratique dans le cadre de projets qui

feront progresser notre industrie sur un sujet concret. Je ne connais pas tous les détails à propos du HDH et n'entends pas trop m'étendre sur ce sujet qui s'est avéré extrêmement sensible, mais je peux témoigner du fait que le HDH a fait le choix de mêler l'utilisation d'un *cloud* Azure qui, visiblement, représentait la solution à ses besoins du moment, à des outils de cybersécurité qui permettent de contrôler les accès, d'identifier les utilisateurs qui accèdent à tel ou tel type de données et de tracer l'activité autour des accès internes à ce *cloud*. Un tel montage ne nous prémunit pas des problématiques juridiques, mais d'un point de vue technologique, il offre tout de même de la visibilité sur les accès aux données stockées dans ce *cloud*. Or, lorsque nous commencerons à sauvegarder des données publiques dans ce *cloud*, nous devrons *a minima* être capables de savoir exactement qui fait quoi et à quel moment, de manière à pouvoir mettre un point d'arrêt aux éventuels accès illégaux ou non appropriés.

Tel est d'ailleurs l'objet du RGPD que de protéger les traitements effectués sur les données et de s'assurer qu'ils sont, au minimum, maîtrisés et anonymisés.

Pr Florence G'Sell. Je souhaite revenir sur le *Buy European Act*. Si celui-ci doit se faire, ce qui, encore une fois, relève plus d'une question de stratégie que de droit, je considère à titre personnel qu'il repose sur une excellente idée, certes évoquée depuis assez longtemps, à savoir une politique européenne qui réserve aux PME européennes une certaine partie des marchés publics.

En revanche, une telle politique menée au niveau national poserait, selon moi, un certain nombre de difficultés au sein de l'Union européenne. C'est pourquoi, il convient avant tout de parvenir à s'entendre à Bruxelles. Je sais bien que les pays du Nord ne sont pas très favorables à ce type d'initiatives. Nous retomberons probablement sur le même genre de difficultés que celles que nous avons pu rencontrer dans le domaine de la fiscalité, mais il me semble difficile, en l'état de nos textes, d'imaginer mettre en place un texte purement national.

En effet, je ne vois pas bien comment nous pourrions initier un tel bras de fer, même si nous nous contentons par exemple de dire que nous ne voulons pas, en France, dans nos appels d'offres, d'entreprises ou de filiales d'entreprises américaines. Cela créerait des difficultés à l'échelle intracommunautaire.

M. Philippe Latombe, rapporteur. En fin d'année 2020 est intervenue la sortie de l'Angleterre de l'Union européenne : y voyez-vous une menace ? En effet, nous avons négocié avec les Anglais un certain nombre d'accords commerciaux qui se substitueront à ceux que nous connaissions à l'époque de l'intégration de l'Angleterre dans l'Union européenne, mais comment devons-nous désormais travailler avec eux ? L'Angleterre servira-t-elle de cheval de Troie aux Américains ? Son départ de l'Union européenne offrira-t-il l'opportunité de continuer à exporter notre modèle ? Je rappelle en effet que nous ne serons plus tenus par le RGPD à compter du mois de juin 2021.

Bref, comment fonctionner avec ce voisin très proche, sachant que les Américains sont plus loin et que les Chinois le sont encore davantage ? Si les Anglais adoptent une législation différente de la nôtre, rencontrerons-nous de nouvelles difficultés ? Quel est votre sentiment sur ce point ?

M. Jean-Noël de Galzain. L'Angleterre constitue le plus gros marché d'Europe en matière d'IT : elle représente en effet 15 % à 17 % du marché européen. Il s'agit toutefois d'un marché très libéral, qui a toujours été utilisé par les fournisseurs américains de solutions

pour s'installer en Europe. Cela ne changera pas, c'est pourquoi la sortie de l'Angleterre ne modifiera pas fondamentalement le *business* des acteurs d'HEXATRUST.

En revanche, sur le plan du RGPD, cette sortie aura probablement un effet au sens où nous devrons nous assurer qu'elle ne permet pas de contourner certaines avancées réglementaires, qui s'avèrent absolument essentielles. Notre collaboration avec les Anglais me semble très bonne en matière de sécurité, tout comme sur certains sujets industriels. Nous devons être inclusifs et travailler ensemble au maximum.

Du point de vue économique toutefois, la sortie de l'Angleterre ne changera pas fondamentalement les choses. L'Angleterre restera un marché indépendant et *american friendly*. Nous sommes présents en Angleterre, le Brexit n'a rien changé à cela.

Pr Florence G'Sell. Nous devons être relativement pragmatiques, au regard des décisions que prendra le Royaume-Uni sur un certain nombre de sujets.

S'agissant des data, la balle est dans leur camp. Si ma mémoire ne me joue pas un tour, en fin d'année, un certain nombre d'éléments de convergence ont tout de même été trouvés autour de la question des data. En outre, l'Union européenne dispose de règles qui conduisent à étudier de manière très pragmatique les garanties offertes par tout pays vers lequel nous serions amenés à transférer des données.

Je pense donc qu'il convient de conserver un tel pragmatisme. S'il s'avère que le Royaume-Uni gomme un certain nombre de ces garanties, il conviendra d'en tenir compte, mais de manière pragmatique, au cas par cas.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder des sujets qui ne l'ont pas encore été, ni dans les propos liminaires ni dans nos échanges ?

M. Stéphane Volant. Quels seraient les critères de souveraineté qu'il faudrait mettre en exergue pour prétendre être souverain et faire de cette souveraineté une valeur ajoutée, de telle sorte que, sans passer par la contrainte, les solutions définies et validées comme souveraines, en France, par un organisme indépendant, puissent être retenues, parce qu'elles sont concurrentielles, sur la base de fonctionnalités identiques, souveraines et protectrices, quitte à ce que leurs prix soient légèrement supérieurs ? Bref, pouvez-vous nous éclairer, en droit, sur les conditions de la souveraineté ?

Pr Florence G'Sell. En réalité, tout dépend de ce que vous entendez par souveraineté. Lorsque vous évoquez la souveraineté, j'entends « souveraineté industrielle ».

M. Stéphane Volant. Vu par l'utilisateur, la souveraineté correspond à un outil qui le met à l'abri de lois et règlements extérieurs, ou encore de poursuites qui ne seraient pas entreprises par l'État français ou par l'Europe et pourraient, de ce fait, être utilisées à des fins de manipulations commerciales, permettant de favoriser un autre pays que le nôtre, voire d'autres entreprises que les nôtres. Mes termes ne sont pas ceux d'un juriste, mais telle est bien l'idée : nous attendons de la souveraineté que les lois françaises et européennes s'appliquent, mais pas les autres, et que, par ailleurs, quelles que soient les conditions du moment, nous puissions continuer à accéder à nos données.

Telle est bien la double dimension de la notion de souveraineté : la protection juridique et du coup, commerciale, et un accès permanent, quelles que soient les conditions du moment.

Pr Florence G'Sell. Votre propos emporte deux aspects. D'abord, nous souhaitons que même les entreprises extérieures à l'Union européenne, à qui nous achetons des services et qui sont installées chez nous *via* leurs filiales, respectent nos règles, ce qui n'est pas toujours le cas aujourd'hui encore, à bien des égards. Toutefois, certains éléments deviennent de plus en plus clairs dans les règlements européens. Ainsi, toutes les dernières propositions de règlements exigent qu'un représentant légal soit désigné, au sein de l'Union européenne, dès lors que vous offrez vos services sur son territoire. Cela peut sembler une évidence, mais ce n'est pas négligeable, vu que, dès que vous arrivez dans l'espace numérique, l'univers virtuel permet de se promener sur la toile indépendamment des assises et emprises nationales. Par conséquent, le fait de disposer de ces *regulatory access points*, c'est-à-dire des personnes qui, au sein de l'Union européenne, répondent des actes accomplis par des entreprises dont le siège se situe à l'extérieur, constitue déjà un point majeur.

Ensuite, le deuxième volet de votre propos a trait à ce que nous venons d'évoquer jusqu'à présent, c'est-à-dire au fait d'essayer quand même d'avoir, en tant que prestataires, non pas des entreprises étrangères dont nous avons envie qu'elles respectent nos règles, mais des entreprises établies en France ou en Europe, respectueuses de nos principes et de nos règles. Cette volonté nous amène à nous demander s'il ne faudrait pas réserver une part de la commande publique à ces entreprises, afin de favoriser leur développement, voire s'il ne faudrait pas déployer des stratégies encore plus agressives afin de les aider, par le biais de « bacs à sable réglementaires » par exemple. Il me semble que nous disposons désormais d'outils d'accompagnement des start-up et des PME dans le domaine du numérique plutôt positifs : nous aidons beaucoup le secteur du numérique, même si ce n'est peut-être pas encore suffisant.

Tels sont donc les deux volets que j'identifie dans votre question : d'un côté, soumettre des entreprises étrangères à notre réglementation et, de l'autre, favoriser nos propres entreprises, notamment celles qui sont vertueuses. De fait, je travaille plus sur le premier point, soit la question de la régulation et du respect de nos règles par ces entreprises étrangères, mais l'autre aspect revêt également de l'importance, au travers de la question du *cloud* souverain et du stockage des data. Nous allons donc développer des solutions de stockage souveraines.

Je souhaite toutefois mettre un bémol sur ces inquiétudes : dans le *Cloud Act*, nous partons de l'hypothèse qu'une entreprise américaine, qui a le contrôle de données pourtant stockées en Europe, ne sera sollicitée par les autorités fédérales américaines pour divulguer des data que dans le cadre d'une procédure bien spécifique. Dans la plupart des cas, l'agence fédérale américaine intéressée par ces data devra disposer d'un *warrant*, qui, par nature, peut être contesté par l'entreprise qui en fait l'objet. Il existe donc tout de même des garanties procédurales. Nous ne sommes pas dans un système où l'administration américaine pourrait venir se servir au prétexte que les données sont hébergées par Microsoft ou par Amazon.

C'est pourquoi, d'ailleurs, nous devons avancer sur les fameux *Executive Agreements* prévus par le *Cloud Act*. Pour le coup, le Royaume-Uni l'a fait, et, dès que nous aurons conclu avec les États-Unis un *Executive Agreement,* comme prévu par *le Cloud Act*, les fournisseurs de services qui sont destinataires des demandes de communication disposeront déjà de plus de facilités pour s'opposer à celles qui viennent des agences américaines.

Je n'ai pas sous les yeux toutes les données chiffrées relatives à ces demandes de communication. Selon des rumeurs, elles auraient explosé auprès d'Amazon ou de Microsoft, mais je ne dispose pas de chiffres précis. Néanmoins, à l'évidence, pour résoudre ce problème, il est certain qu'il convient d'en passer par un *cloud* souverain : j'ai par exemple eu

l'occasion d'échanger avec la DGFiP qui dispose actuellement de systèmes de stockage très élaborés. Rien ne nous empêche donc d'avancer maintenant que GAIA-X est en place.

J'ai davantage étudié la question de la régulation des immenses plateformes et entreprises, dont nous avons l'impression qu'elles sont actuellement en train de tout capter, comme en atteste la spectaculaire réussite d'Amazon et son efficacité particulièrement impressionnante. Or nous avons tout de même largement avancé à cet égard au travers des derniers projets de textes, puisque les deux projets de règlements publiés par la Commission avant Noël s'avèrent extrêmement bien pensés et très complets.

Je souhaiterais d'ailleurs faire quelques remarques à leur propos. Tout d'abord, nous avons enfin compris qu'il nous faut réguler de manière asymétrique : le modèle d'affaires des très grandes plateformes s'avère en effet très particulier, au sens où non seulement elles fournissent l'architecture, mais elles interviennent sur celle-ci pour faire concurrence à des vendeurs professionnels (ce qui est le cas d'Amazon qui propose ses propres produits sur sa propre plateforme). Or nous sommes parvenus à aborder la spécificité de ce modèle d'affaires.

Ensuite, il me faut tout de même soulever une difficulté, à savoir la question des moyens humains. J'ai en effet eu la chance de participer à un petit projet de recherche, l'année dernière, au cours duquel nous avons interrogé un grand nombre de start-up du numérique. Toutes ont exprimé le reproche suivant : que ce soit en France à l'égard de la CNIL ou à l'égard de la Commission européenne, elles attendent trop pour connaître l'interprétation de telle ou telle nouvelle norme, de telle ou telle exigence du RGPD, et obtenir une réponse de la part de leur interlocuteur. Ce reproche pose donc la question des moyens humains et des compétences que peuvent mobiliser les autorités de régulation, au niveau national comme au niveau européen. Il s'avère donc extrêmement positif de disposer désormais de régulations bien pensées, mais encore faut-il les mettre en œuvre dans des délais raisonnables et d'une manière qui sécurise les acteurs.

Par ailleurs, nous avons besoin de préciser très rapidement le contenu des obligations mises en place : le *Digital Market Act* emporte ainsi des obligations dont il est dit qu'elles seront ultérieurement précisées par la Commission. Il s'agit vraiment d'un important enjeu de sécurité juridique.

La question des acquisitions est également évoquée dans le *Digital Market Act*. Or, dans le secteur du numérique, le scénario des *killer acquisitions* s'avère parfaitement connu : de jeunes pousses innovantes, disruptives et prometteuses, qui fonctionnent bien et font parler d'elles, sont rachetées à prix d'or par un géant de l'Internet. Il s'agit d'une énorme difficulté, car, bien entendu, de telles offres de rachat mirobolantes s'avèrent particulièrement tentantes. C'est pourquoi le *Digital Market Act* emporte, pour toute acquisition de cette nature, une obligation de notification à la Commission. Cependant, aucun mécanisme n'est ensuite prévu, si les seuils du droit antitrust n'ont pas été atteints. Il me semble donc que nous ne sommes pas allés jusqu'au bout de la logique, à moins que la Commission en tienne compte dans la définition des obligations qui pèseront sur les grandes plateformes. Ce problème me semble devoir être étudié, car il est important que nos jeunes pousses les plus prometteuses ne soient pas systématiquement rachetées par des géants technologiques.

Enfin, je souhaite évoquer la question de la coopération à l'échelle européenne. En effet, parce qu'il s'adresse aux très grandes plateformes, le *Digital Market Act* désigne la Commission en tant qu'autorité de contrôle, tandis que, dans le *Digital Services Act*, comme dans d'autres textes européens, les autorités nationales, réunies au sein d'un comité européen sur les services numériques, conservent la main. Ce comité de coordination répond bien

entendu à d'importants enjeux politiques, mais comment l'articuler avec les autres autorités pour aboutir à un dispositif qui fonctionne mieux et plus vite ? Est-il complètement exclu de constituer une autorité de contrôle numérique à l'échelle européenne ? J'ai en effet le sentiment qu'en matière numérique, il convient de raisonner d'abord à l'échelle européenne.

Pour finir, un programme de commande publique dans le monde numérique s'impose selon moi pour aider nos entreprises, accompagné d'une vraie transformation numérique des administrations.

M. Philippe Latombe, rapporteur. Vous indiquez que les deux prochaines directives européennes n'emportent aucun volet relatif aux acquisitions. À l'inverse, nous avons la capacité de contrôler les acquisitions d'entreprises de défense. Par conséquent, faut-il transposer au numérique les règles appliquées dans le domaine de la défense, soit des critères très précis en termes de capacités technologiques et d'avantages compétitifs, ou bien construire une réglementation plus large qui toucherait toute forme d'entreprise, même en dehors du numérique ? Vous avez déjà fait référence au rachat d'Alcide par un géant américain et des interrogations demeurent à propos du projet de rachat d'ARM par Nvidia, sachant que, pour ces derniers, l'argent n'est pas le nerf de la guerre. Faut-il mettre des barrières et comment ?

M. Stéphane Volant. Parce que je siège au conseil de surveillance de Photonis, je connais bien le dossier. Si je respecte bien entendu les décisions de l'État en matière de souveraineté et l'appelle même, depuis le début de notre échange, à poser des règles, je pense néanmoins que ces règles doivent être, dès le départ, extrêmement claires et listées de manière exhaustive, afin que nul ne puisse les ignorer. En outre, l'autorité chargée de les faire respecter doit vraiment être celle qui les fait respecter. En effet, dans certains dossiers, que vous venez de citer, les règles n'étaient pas très précises au départ, elles pouvaient être interprétées de manière différente et les autorités chargées de les faire respecter n'ont pas toujours été celles qui les ont fait respecter *in fine*.

En matière numérique, j'appelle donc de mes vœux de vrais critères de souveraineté, même si, pour le moment, je ne sais ni où ni ce qu'ils sont. Ces critères doivent être listés de manière exhaustive et une unique autorité doit être, à la fois au début et en cours de *process*, chargée de les faire respecter. Nul ne doit pouvoir ignorer leur existence et une seule autorité doit être fondée à les faire appliquer. En effet, comme l'indiquait le Commissaire général au Plan, François Bayrou, « trop de souveraineté tue la souveraineté ». Nous ne sommes pas un village gaulois, nous appartenons à l'Europe, nous commerçons avec des étrangers et devons donc veiller à faire strictement respecter ce qui est un bien commun et que nous n'avons pas envie de voir dégrader par d'autres.

M. Jean-Noël de Galzain. Pour moi, ce n'est pas en contraignant très fortement les fonds d'investissement ou autres que nous réussirons à régler ces problématiques de souveraineté. Ce n'est pas non plus en essayant de brider des velléités capitalistiques autour de start-up, PME ou ETI. Il existe en effet des investisseurs financiers et industriels qui ont envie de réaliser, tandis que d'autres mettent plus de temps ou n'en ont pas envie. Telle est la liberté de chacun : d'ailleurs, tous les exemples d'interventionnisme auprès de start-up ou PME ont peu ou prou abouti à des faillites, voire à la décrépitude des entreprises retenues contre leur gré. Je ne crois donc pas à ce principe.

En revanche, il me paraît urgent de considérer le fait qu'un certain nombre d'entrepreneurs ne sont pas attirés par l'idée de devenir milliardaires à tout prix. D'aucuns associent le profil du patron à la volonté de « s'en mettre plein les poches », mais il faut avoir

à l'esprit qu'un certain nombre d'entrepreneurs sont séduits par l'idée de créer des géants mondiaux comme Schneider Electric, Alstom et d'autres sociétés françaises qui ont fantastiquement bien réussi. Or, pour y parvenir, ils ont besoin d'un certain nombre d'instruments qui fonctionnent, à savoir des solutions de sortie pour les investisseurs, c'est-à-dire des solutions permettant de réaliser, sans avoir à revendre là où les capitaux sont les plus nombreux, là où ils s'achètent le plus cher.

Par conséquent, un important travail reste à accomplir afin que les bourses européennes reprennent de la valeur et que les marchés financiers soient alimentés par des capitaux autour de belles histoires industrielles européennes. Le Nasdaq ne constitue pas l'unique modèle ; il faudrait que nous disposions d'un Nasdaq européen. De belles histoires peuvent se réaliser en Europe : des entreprises de cybersécurité, des entreprises numériques, des entreprises spécialisées dans les nouvelles industries pourraient y trouver des débouchés. Enfin, il convient de proposer des instruments capitalistiques permettant de réaliser des acquisitions dans de telles entreprises stratégiques. Il est ainsi tout à fait possible, à l'échelon européen, de mettre en place des poches de financement dédiées, dans un environnement de partenariat stratégique entre le privé et le public.

Pour finir, après avoir entendu la définition juridique de la notion de souveraineté, je préciserai que le numérique recouvre à la fois le *cloud*, la cybersécurité, les technologies quantiques, l'intelligence artificielle et la robotique, soit des sujets qui ont trait à l'indépendance de la France. Qui aurait pu imaginer la pandémie que nous connaissons aujourd'hui et notre actuelle dépendance aux vaccins ? Quel juriste ou politique aurait pu l'anticiper ? Nous sommes dans un tel état de dépendance qu'il est urgent de mettre en place nos propres territoires numériques, afin de bénéficier d'une vraie autonomie dans un certain nombre de domaines, dont le numérique sera à la fois le moteur et le garant. Il s'agit d'une urgence au service de notre autonomie stratégique. Je mets donc volontairement de côté les problématiques de nationalités, dans ma définition de la souveraineté.

Pr Florence G'Sell. Je suis très sensible à ce que vient de dire M. Jean-Noël de Galzain : effectivement, nous n'allons pas nous mettre à empêcher les entrepreneurs de vendre leurs biens. Je m'étonne cependant que le *Digital Market Act* impose une forme de notification de toute opération de concentration dans le secteur des services numériques, sans que nous en tirions grand-chose, ce qui pose un problème de cohérence, tandis que nous nous apprêtons à adopter un texte qui prévoit tout de même de contraindre les géants du numérique à céder une partie de leur activité, s'ils ne respectent pas leurs obligations.

Il s'agit donc pour moi d'un sujet à suivre. Nous avons prévu une notification, la Commission va donc surveiller, mais faut-il en complément étendre des règles déjà existantes par exemple dans la loi PACTE, s'agissant des industries stratégiques ? Je demeure partagée.

M. Stéphane Volant. La souveraineté numérique doit devenir un avantage concurrentiel pour les solutions françaises et européennes. Or un avantage concurrentiel ne se décrète pas. Nul ne peut légiférer sur un avantage concurrentiel : il se gagne.

Nous mettre dans les conditions de faire gagner les solutions françaises, parce qu'elles ont des critères de souveraineté, qui, dès lors, apparaissent comme un avantage concurrentiel, correspond en réalité à ce que nous recherchons tous. Pour ce faire, le meilleur des moyens demeure un législateur qui, comme vous l'avez fait aujourd'hui, écoute les utilisateurs et les industriels (grands, petits et moyens), et s'appuie sur des expertises juridiques.

Comme vous l'aurez constaté, nous sommes plutôt d'accord sur ce point : nos propos de ce jour constituent presque un « prêt à voter ». Je voudrais donc, en guise de conclusion, vous remercier de nous avoir réunis tous les trois, car il est rare que nous ayons l'occasion d'intervenir ensemble. Au nom de quelques-uns des grands utilisateurs de solutions numériques, je vous remercie d'avoir mis ces questions en lumière. Mettez-nous maintenant en position de gagner notre avantage concurrentiel ; la filière des industries de sécurité s'avère prête à remporter ce pari. La France a quelques atouts, mais il ne faut pas traîner, car nous sommes, à date, encore très en retard.

M. Philippe Latombe, rapporteur. J'ai bien entendu l'urgence que vous exprimez. Échanger avec vous sur ce sujet était très intéressant. Nous avons besoin de vos retours et ne pourrons rien faire contre vous, c'est aussi pourquoi ces auditions sont diffusées, voire ouvertes à la presse, lorsqu'elles sont publiques.

Je vous invite à nous envoyer des contributions, si vous affinez vos réflexions, afin que nous puissions les intégrer au fur et à mesure. Si, au cours d'une audition, vous repérez un propos sur lequel vous souhaitez réagir, parce qu'il s'agit d'une mauvaise idée, ou insister, parce qu'il s'agit d'une bonne idée à creuser, n'hésitez surtout pas, car nous avons besoin de vos réactions. Notre mission se prolonge durant un an, afin que, sur ce temps long, nous soyons en mesure de ne pas commettre d'erreur, l'urgence du sujet nécessitant de notre part une très grande précision.

M. Jean-Noël de Galzain. Il nous faut toutefois réagir d'ici la fin de l'année 2021.

M. Philippe Latombe, rapporteur. Notre mission a débuté en juillet 2020 et doit rendre son rapport en juin 2021

M. Jean-Noël de Galzain. Nous pourrions, si vous le souhaitez, revenir sur vos travaux dans la configuration de ce jour. Nous vous enverrons le Manifeste. Nous sommes un pays d'entrepreneurs et vous devez savoir que, pendant la crise, les entrepreneurs se mobilisent pour tenir leur moral et celui de leurs employés, mais aussi tenter de faire grandir leurs entreprises dans un environnement difficile.

Les entrepreneurs ont vraiment besoin d'être encouragés dans l'idée qu'il est encore possible de rêver et de réussir dans notre pays et sur notre continent, sans avoir à aller chercher « le gros chèque » ailleurs. L'éducation, l'enseignement supérieur, nos aînés, comme les utilisateurs sont tous mobilisés en faveur de la création de valeur et capables des plus grands exploits, mais il convient tout de même de se poser la question de l'exécution : pour une fois, faites les choses avec nous ! Permettez-nous de rêver au fait qu'il est possible, dans ce pays et sur le continent européen, de créer un nouvel Airbus dans le domaine du numérique ou de la cybersécurité ! Telle est la volonté des entrepreneurs du regroupement HEXATRUST.

M. Philippe Latombe, rapporteur. Je vois bien que les entrepreneurs font tout leur possible pour aider l'ensemble des citoyens à surmonter la crise. Notamment dans le domaine du numérique, nombre d'initiatives ont vu le jour, au titre desquelles nous devrons remercier l'ensemble des écosystèmes. Si notre mission peut, à sa mesure, vous aider, elle le fera avec le plus grand des plaisirs.

La séance est levée à treize heures.

Membres présents ou excusés

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

Réunion du jeudi 11 février 2021 à 11 heures

Présents. - M. Philippe Latombe, M. Jean-Luc Warsmann

Excusée. – Mme Frédérique Dumas