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
9 février 2021
Séance de 11 heures

Compte rendu n° 26

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, *rapporteur*

ASSEMBLÉE NATIONALE

Audition commune de Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE, M. Michel Paulin, directeur général d'OVHcloud, et Mme Karine Picard, directrice générale d'Oracle France

La séance est ouverte à 11 heures.

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Nous démarrons aujourd'hui un cycle d'auditions consacrées au *cloud* et à la protection des données. Nous recevrons jeudi prochain les représentants d'Hexatrust, du Club des Présidents de sécurité et de sûreté des entreprises (CDSE) et du Club des juristes, avant d'échanger la semaine suivante avec l'ensemble des acteurs du numérique en santé. Pour lancer ce cycle, nous recevons aujourd'hui plusieurs entreprises importantes dans le domaine du *cloud*. Participent à cette table ronde numérique Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE, M. Michel Paulin, directeur général d'OVHcloud et Mme Karine Picard, directrice générale d'Oracle France.

En introduction, nous souhaiterions vous entendre sur trois sujets. Comment, en tant qu'entreprise privée spécialisée dans le domaine du *cloud*, percevez-vous la montée en puissance du thème de la souveraineté numérique dans le débat public ? Sur ce premier sujet, je résumerai mon propos en deux courtes questions. Comment appréhendez-vous la notion de souveraineté numérique française ou européenne ? Et de quelle façon pouvez-vous participer à sa protection/promotion en tant qu'entreprise privée ?

J'aimerais également que vous nous décriviez votre vision de l'état actuel du marché mondial du *cloud*, qui est dominé par quelques géants du numérique, parmi lesquels Google, Microsoft et Amazon. Je souhaiterais que vous nous rappeliez quels en sont les différents segments et la place des acteurs européens. Je suis également intéressé par votre regard sur les pratiques des entreprises du secteur public vis-à-vis du recours à des solutions *cloud* et sur les principales tendances qui pourraient émerger sur ce marché, dans les prochaines années.

J'aimerais enfin savoir ce que vous pensez du cadre juridique européen actuel, entourant la question des données, avec le Règlement général sur la protection des données (RGPD), et du cadre futur, avec ,outre le *Digital Services Act* (DSA) et le *Digital Market Act* (DMA), une proposition de règlement de la Commission européenne concernant la gouvernance des données, appelé également *Data Government Act*. Selon vous, le bon équilibre a-t-il été trouvé entre la nécessité de soutenir l'innovation, la donnée étant devenue le « nouveau pétrole de l'économie numérique », et la protection nécessaire des données des utilisateurs et de la souveraineté des États et de l'Union européenne ? En outre, comment peut-on assurer un niveau maximal de sécurité pour les données dans un contexte de sophistication de la menace cyber ?

Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE. 3DS OUTSCALE est le *cloud provider* de Dassault Systèmes. Notre entreprise a 10 ans. Elle regroupe 160 collaborateurs. C'est la filiale d'un très grand groupe, puisque Dassault Systèmes vient d'annoncer un chiffre d'affaires de plus de 4,5 milliards d'euros pour 2020. Nous sommes éditeurs de notre propre solution d'orchestration de *cloud*, ce qui est important par rapport aux différents sujets que nous aborderons et par rapport à la maîtrise que l'on peut avoir de son avenir dans le *cloud*. Nous sommes particulièrement positionnés sur le domaine

de la confiance, voire de l'hyper-confiance, avec des solutions très industrialisées depuis le départ. Nous sommes un acteur du *BtoB*.

Nous avons, dès le départ, fait le choix d'avoir une activité complètement programmatique, accessible par *API* (pour *Application Programming Interface* dans le jargon de notre secteur d'activité), très processée et industrielle, avec l'ensemble de nos offres au périmètre Iso 27 001 depuis 2014. Nous avons également très tôt fait le pari du plus haut niveau de certification. Cela nous paraît le meilleur moyen pour gagner la confiance des clients et faire en sorte qu'ils fassent le pas de migrer vers le *cloud* (à la fois les clients privés et les administrations). Nous avons eu le plaisir d'être les premiers fournisseurs d'infrastructures réseau service à obtenir la qualification SecNumCloud, qui correspond au référentiel de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Nous avons été récemment rejoints par nos amis d'OVH. Nous avons passé la certification « hébergeur de données de santé » qui permet de nous tourner vers le secteur de la donnée de santé qui pèse lourd dans le registre des données sensibles.

S'agissant de la définition de la souveraineté du *cloud* et du retour du terme de souveraineté par rapport aux activités numériques, nous le vivons avec beaucoup d'intérêt et de satisfaction. En effet, nous sommes sur ce créneau depuis le départ. J'ai oublié de préciser que nous sommes également présents aux États-Unis et en Asie, au Japon notamment, en mode multi-local. C'est-à-dire que, quelle que soit la région où nous sommes présents, nous garantissons à nos clients la souveraineté de leur relation avec nous.

Pour nous, la souveraineté du *cloud* est la garantie que les données seront stockées en France pour la souveraineté française, qu'elles seront également opérées en France, et qu'il n'y aura pas d'aller-retour de la donnée vers des serveurs sans que nous sachions où et à quel moment. Il s'agit d'un contrat signé avec les entreprises en droit français, ce qui est très important pour la vie de la relation contractuelle avec nos clients, avec un support de proximité 24/7 qui est opéré en anglais et en français. La relation de proximité est assurée par des équipes basées en France. Dans le contexte réglementaire actuel, la souveraineté s'entend du fait de n'être absolument pas soumis à des réglementations extra-européennes. J'entends par là que l'on ne peut pas prétendre être souverain si l'on est soumis au *Cloud Act*.

Aujourd'hui, après avoir été pas mal galvaudé, voire un peu tabou pendant quelques temps, le mot revient fortement. Après la promulgation du *Cloud Act* en 2018 et après que le confinement a révélé que la France et l'Europe étaient dépendantes de beaucoup de continents sur de nombreux sujets, dont le numérique, il est très important et très agréable, pour nous qui apportons des solutions souveraines, de voir que le sujet revient sur le devant de la scène et que les entreprises et les administrations se mobilisent pour essayer de faire en sorte que les offres souveraines existent et perdurent.

Nous travaillons, notamment avec M. Michel Paulin, au sein du Comité stratégique de filière, pour pousser ces notions de souveraineté et pour faire en sorte que la filière puisse avancer. Dans le cadre de ce Comité stratégique de filière, nous avons signé un contrat avec les ministères. Nous attendons des engagements forts de l'État sur le fait de réglementer la nécessité d'utiliser un *cloud* de confiance pour les données sensibles pour les administrations et les opérateurs d'importance vitale (OIV). Il est nécessaire d'impulser un mouvement fort pour les administrations et les grandes entreprises d'importance vitale en France. Il y a deux volets. Le premier est le fait de réglementer les choses. La bonne nouvelle est que le Cigref a réalisé une étude récemment. Les membres du Cigref sont prêts à accepter une réglementation supplémentaire parce que les enjeux leur paraissent primordiaux. Le

deuxième volet concerne la mise en place d'un label permettant de définir ce qu'est un *cloud* de confiance. Aujourd'hui, le référentiel SecNumCloud porte essentiellement sur les critères techniques. Il en va de même pour le référentiel HDS pour l'hébergement de données de santé. Ces référentiels, labels, ou qualifications n'emportent jamais cette logique que son détenteur n'est pas soumis à des lois extra-européennes. Cela manque dans le paysage. Il faudra y travailler rapidement. Il faut pouvoir dire : *« Nous, qui répondons aux critères que je vous ai donnés tout à l'heure, nous pouvons l'exposer publiquement, parce qu'une entité publique nous donne le droit de le faire »*. Il sera également très important, dans le cadre de Gaia-X, qui créera des standards à l'échelle européenne, de faire ressortir, au sein des offres qui vont adopter des standards techniques, celles qui sont de confiance au sens où elles garantissent la souveraineté.

Mme Karine Picard, directrice générale d'Oracle France. La société Oracle est une société américaine, dont le siège est à Austin au Texas, qui est implantée en France depuis trente ans. Je suis la partie hors France de ce débat. Oracle fait partie des cinq grandes sociétés qui fournissent des *clouds* dans le monde. Vous avez cité les trois premières qui ont une énorme part de marché. Depuis plus de trente ans, nous fournissons des solutions à la fois à l'État, puisque nous sommes présents dans tous les ministères régaliens : la santé, l'armée, le ministère de la Défense, de l'Industrie, de l'Économie. Nous connaissons les enjeux en termes de sécurité au niveau de l'État, mais aussi dans les grandes entreprises françaises, et depuis peu, dans tout ce qui est Next 40.

Aujourd'hui, Oracle fait face à une montée de la souveraineté, pas uniquement en France. Nous le constatons depuis cinq ans dans plusieurs pays, même en Angleterre. Même s'il est extrêmement proche des États-Unis, ce pays est très souverain en ce qui concerne ses données. Nous observons une même émergence en Allemagne, en France, dans les pays du Nord, au Moyen-Orient. Cette résurgence de la souveraineté n'est pas nouvelle. Depuis de nombreuses années, en tant qu'éditeurs américains, nous avons pris conscience de cette demande et nous y avons travaillé sur deux angles. Le premier est d'être capable de fournir des offres de *cloud* public, les données étant hébergées en Europe au départ, en respectant tout ce qui est RGPD. Le deuxième est la volonté d'investir pour disposer de centre de sonnées (*data centers)* présents dans les pays. Nous aurons un *data center* en France, dans les mois qui viennent, à Marseille. Cette demande de stocker les données, au-delà de la signature de contrats avec une société française, s'est accélérée ces dernières années. C'est pour cela que nous investissons en Suède et en Italie.

Nous ressentons véritablement cette résurgence de la souveraineté. En revanche, cela n'a pas empêché les grandes entreprises françaises d'adopter le *cloud* depuis huit-dix ans. 43 % des sociétés du CAC40 utilisent déjà des solutions Oracle *cloud* ou autres, et un peu plus de la moitié, en termes de technologies ou d'infrastructures. Les grandes entreprises publiques, pour un certain nombre de leurs processus métiers (finance, RH, marketing, recrutement, infrastructures), utilisent les entreprises qui respectent les règles de souveraineté. Il s'agit aujourd'hui d'une accélération. Comme Mme Servane Augier le disait, il est vrai qu'avec le Covid, la demande du *cloud* est accrue, ce qui génère un volume plus élevé de données, de transactions, de points d'entrée. Cela a découvert des brèches de sécurité potentielles dans certains systèmes. Certaines entreprises se sont aperçues qu'elles n'étaient pas très bien équipées en termes de cyber sécurité. Nous observons, de la part des entreprises, une demande accrue de consommation du *cloud*, dans tous les domaines, ainsi qu'une demande accrue de respect d'un certain nombre de critères de sécurité.

Nous sommes aussi certifiés sur les données de santé aujourd'hui. Nous travaillons avec l'ANSSI pour être certifiés SecNumCloud. Nous espérons être un acteur américain qui pourra entrer dans les critères de ce qu'est un *cloud* de confiance. La notion de *Cloud Act* est assez déterminante. Il est important de savoir que le fait qu'un éditeur soit national ne signifie pas qu'il respecte les critères de sécurité. Des investissements doivent être réalisés dans la manière dont sont construits les *clouds*, dans la manière dont on peut contrôler l'ensemble de la chaîne du cloud (depuis la création de la machine, de la puce, de la base de données, des transferts de la donnée, du *data center*). Ce contrôle de la chaîne complète de la donnée est extrêmement important pour assurer la meilleure sécurité. Devant cette demande de souveraineté de nos clients et en particulier des gouvernements, nous avons travaillé sur de nouvelles offres de *cloud*, que l'on appelle des *clouds* régionaux, qui permettent aux gouvernements ou aux entreprises de disposer, derrière leur pare-feu, de tous les avantages du *cloud* public, en termes de consommation de services, d'innovations, mais aussi de protection des données. Ainsi, pour répondre à votre question, en tant qu'acteur du *cloud* et en tant qu'acteur américain, cela fait plusieurs années que nous travaillons à comprendre les besoins des entreprises privées et publiques en France et en Europe, et de répondre à leurs attentes.

Nous sommes membres de Gaia-X depuis le premier jour, puisque nous pensons qu'il faut un cadre qui définisse les critères de sécurité que chaque entreprise doit respecter pour être considérée comme un *cloud* de confiance. Aujourd'hui, la crise l'a révélé, mais c'est une évidence : tous les secteurs de l'informatique ne sont pas présents en Europe. Nous avons la chance d'avoir en France des fournisseurs de *cloud* qui sont des opérateurs de *clouds* puissants. Cependant, un certain nombre d'opérateurs métiers n'existent pas. Il est important de pouvoir créer une interopérabilité des *clouds* pour les entreprises et pour le Gouvernement, parce que l'ensemble des fournisseurs de services n'existe pas aujourd'hui en Europe. Il faut mettre cette structure en place pour garantir la sécurité des données. Voilà ce que je peux dire en tant qu'Oracle France aujourd'hui, avec ses 1 300 employés sur le territoire, qui n'ont qu'un objectif : servir et protéger l'ensemble des clients français.

M. Michel Paulin, directeur général d'OVHcloud. OVHcloud est un opérateur de *clouds*. Nous sommes classés, par les analystes, comme faisant partie des dix plus grands mondiaux, même si, bien entendu, nous sommes plus petits à l'échelle des *hyperscalers*. Nous nous adressons aujourd'hui à tout type de clients. Historiquement, nos clients étaient plutôt des sociétés Tech, ce que nous appelons dans le jargon les *digital natives*. Depuis quelques années, nous avons l'ambition de nous tourner aussi vers le marché des grandes entreprises, des grandes administrations, des collectivités publiques ou privées.

Quels sont les grands principes d'OVHcloud aujourd'hui ? Le premier est que nous défendons un *cloud* de confiance, par définition technique et par définition légale, dans le sens où techniquement, nous sommes un grand supporter de l'*open source*. Nous travaillons sur des solutions interopérables, ouvertes, réversibles. L'interopérabilité est clé. Pour cela, il faut garantir que les *API* soient documentées, ouvertes, qu'il s'agisse des *API* au-dessus ou en dessous. Il faut faire en sorte que l'ensemble des solutions logicielles soient réversibles. Nous avons aussi une longue tradition d'intégration avec un modèle. Nous construisons nous même nos serveurs. Cela donne une totale traçabilité en France, à partir de composants qui sont achetés à travers le monde. Nous avons aussi la volonté de travailler avec un écosystème. Cet écosystème sera un moyen pour dynamiser la filière européenne et la filière française. Nous investissons massivement. Nous sommes 2 300 aujourd'hui à travers le monde. Nous investissons dans nos 32 *data centers*. Nous venons d'ouvrir un *data center* en Asie, à Singapour, et un autre, à Sydney. Nous investissons dans la Recherche et Développement. Nous avons, comme l'a mentionné Servane Augier, reçu de nombreuses certifications dont

tout récemment SecNumCloud, mais également les certifications HDS, Iso 27 001. Nous sommes convaincus qu'OVHcloud a les moyens de proposer des solutions alternatives autour du *cloud* de confiance.

Qu'est que la souveraineté ? Pour nous, la souveraineté n'est pas le nationalisme, le patriotisme, le protectionnisme, mais la capacité pour des États, pour des entreprises, pour des individus, de pouvoir choisir. À la fois en termes légaux, techniques, et de pratiques concurrentielles, certains acteurs ont tendance à créer des monopoles fermés, qui bloquent les clients dans des systèmes. C'est l'inverse de ce que nous pensons être la souveraineté.

Ensuite, nous distinguons la souveraineté des données et la souveraineté des technologies. Cette dernière consiste à se demander si, aujourd'hui, les technologies sont sur des R&D européennes ou françaises. Nous essayons toujours de les défendre, puisque nous sommes une société française et européenne et que nous pensons que les valeurs européennes sont exemplaires, à travers nos choix pour nos partenaires. Mais cela n'est pas exclusif. L'Europe n'a pas la totalité des technologies disponibles dans le domaine du *hardware*, par exemple. Nous pensons qu'il faut que des acteurs comme nous, nous associions à des acteurs pour proposer des solutions. Même si nous essayons de favoriser et de privilégier les technologies européennes, force est de constater que la souveraineté européenne ne peut pas être exclusive.

En revanche, sur la partie relative à la donnée, l'Europe est en avance, à travers le RGPD, à travers *Schrems* II. Nous pensons qu'à ce niveau, il n'y a pas de compromis à faire. Ces sujets sont, pour les domaines européens, des prérequis absolus sur la notion de souveraineté et de confiance. Nous militons depuis de nombreuses années, à travers le comité stratégique de filière (CSF). Nous sommes convaincus qu'il est important de les mettre en avant pour deux raisons. La première est que les entreprises le demandent. Nous le constatons. Comme Servane Augier l'a mentionné, le Cigref a réalisé un sondage auprès des grandes entreprises, lequel a démontré que la notion de souveraineté était une demande de leur part. Il y a des enjeux technologiques, géopolitiques, financiers, un manque de liberté de choix en raison d'un certain nombre de pratiques techniques ou commerciales qui enferment les personnes. Le *cloud* ne doit pas devenir une prison. Il existe une vraie demande des grandes entreprises de garantir la souveraineté. La deuxième raison est la prise de conscience par les citoyens. Nous avons mené un sondage représentatif de citoyens avec l'IFOP pour leur demander ce qu'ils pensaient de la souveraineté des données. 69 % des Français estiment que c'est important. 2 % font confiance aux fournisseurs de *clouds* étrangers. Ils sont extrêmement attentifs sur les domaines de la santé, des données financières, des données publiques. Ils estiment que les données doivent être en France ou en Europe et qu'il doit y avoir une garantie que les acteurs ne puissent pas faire circuler ces données ou métadonnées. Ce sujet ne concerne pas uniquement les acteurs. Nous voyons bien que les clients et les citoyens sont également concernés par ces sujets de confiance. D'une certaine façon, tous les débats passés sur la localisation des données, leur traitement, leurs flux, et l'impact de *Schrems* II démontrent que ces sujets sont d'actualité et impactent les vies des entreprises et des citoyens.

Quels sont les modèles sur lesquels nous nous basons ? Le premier est qu'il est nécessaire de clarifier l'ambition d'un *cloud* de confiance. Nous sommes très fiers d'avoir la qualification SecNumCloud. C'est un gage technique. En revanche, il est très important que nous soyons capables de créer, pour les entreprises et pour les citoyens, des certifications qui garantissent, au-delà des sujets techniques de sécurité, la souveraineté. Où sont les données ? Comment sont-elles transférées ? Quelle est la juridiction ?

Il convient d'être extrêmement précis sur quatre éléments :

– Les données et les métadonnées sont-elles situées dans les *data centers* en Europe ?

– Sont-elles accessibles par des législations de pays hors de l'Union européenne (ce qui est interdit par *Schrems* II) ?

– Le fournisseur *cloud* est-il soumis à la juridiction de l'Europe et exempté des droits extraterritoriaux (en particulier le fameux *Cloud Act*) ?

– La politique du fournisseur *Cloud Act* répond-elle aux demandes d'autorisation des pays tiers conformes au RGPD ?

Ces quatre critères sont extrêmement importants et doivent être ajoutés à toutes les notions de certifications, de labels, pour apporter de la confiance et de la crédibilité à la souveraineté. Par exemple, nous recommandons que le référentiel HDS inclue ces critères. Ce ne sont pas uniquement des critères techniques, mais des critères qui permettront de rétablir la confiance auprès des citoyens et des entreprises. Avec Servane Augier, nous militons pour créer un label *Open Trusted Cloud*. L'État, la Commission européenne devront définir les critères, qui sont très importants pour aider les entreprises à obtenir une clarification et que cela soit labélisé.

Un autre élément important concerne la nécessité d'avoir une clarification à travers l'ensemble de l'écosystème, en particulier avec les éditeurs de logiciels, les fournisseurs de SaaS. Il est utile d'avoir une totale transparence. Celle-ci est un des engagements forts de Gaia-X. Lorsqu'un éditeur de logiciel est en mode SaaS, il doit indiquer quel est aujourd'hui l'hébergeur de *cloud* dans lequel il met sa solution, où sont les données et les métadonnées, quelles sont les conditions juridiques qui protègent ou non. Il est important que l'ensemble de la filière digitale soit transparente et fournisse les garanties à l'ensemble des utilisateurs finaux, les citoyens ou les entreprises. La sensibilisation sur ces sujets nous semble très importante.

Les prises de parole de la CNIL et des différentes CNIL européennes prouvent qu'il n'y a pas cette transparence, aujourd'hui, dans un certain nombre de cas. Dans le cadre de la filière, dans le cadre de Gaia-X, mais également dans le cadre du développement de nos propres solutions, nous serons très vigilants pour proposer à nos clients, à l'ensemble des administrations, une transparence totale sur les conditions d'accès et de protection des données. Tel est notre positionnement.

Avec d'autres acteurs de la filière, OVHcloud continuera à demander à l'État d'être exemplaire. L'État n'est pas exemplaire aujourd'hui. Les collectivités locales ne le sont pas, parfois par ignorance. Il y a besoin d'ouverture. Sur l'UGAP, un certain nombre de critères (où sont les données ? comment sont traitées les données ?) n'apparaissent pas comme des critères de choix pour les collectivités locales, pour les administrations, pour les entités publiques. Nous pensons qu'il est indispensable, de la même façon qu'il existe une traçabilité sur l'alimentation, l'environnement, de donner la visibilité complète, à travers un portail. Il est nécessaire de clarifier dans quelles conditions les logiciels sont hébergés. Après, les clients choisiront en toute connaissance de cause. Aujourd'hui, l'État n'est pas exemplaire. Les conditions d'attribution par les collectivités locales ne sont pas totalement transparentes et ne suffisent pas. Il est important que l'État clarifie sa stratégie et définisse sa doctrine, qu'il clarifie les conditions d'accès des citoyens aux données et fasse évoluer la réglementation.

Nous appelons de nos vœux, à travers le CSF, une loi permettant de clarifier les conditions d'accès aux données sensibles pour les entreprises et les citoyens, une modification des notions de certification pour y ajouter les sujets autour du droit et de la conformité au RGPD.

En dernier lieu, il est très important que l'État soutienne ceux qui, aujourd'hui, respectent les règles. Nous ne cherchons pas des subventions, mais nous cherchons des commandes, comme le font tous les autres. Comme l'a dit Karine Picard, la souveraineté est un sujet qui apparaît partout dans le monde, au Japon, en Inde, en Russie, en Chine bien entendu, aux États-Unis. Tous les acteurs continentaux aident leur filière à respecter les législations locales à travers des commandes. Aujourd'hui, 70 %, voire plus, du total des investissements de technologie de l'information (IT) passent par des acteurs qui ne sont pas européens. C'est 90 % dans certains domaines.

Il est regrettable que l'Europe ne se dote pas d'une filière tout autant aidée que les autres régions, qui aident par la commande publique. C'est d'autant plus important dans le cadre de la crise Covid. Nous avons fait face. Nous avons été capables de répondre à l'enjeu de la digitalisation des entreprises. Le *cloud* que nous représentons, avec Servane Augier, en Europe, a tenu, a été capable de répondre à la demande. Nous avons participé à l'effort de solidarité demandé par le Gouvernement, avec notre initiative *Open Solidarity*. Nous avons embauché en France pour pouvoir construire plus de serveurs, développer notre activité. L'État doit être exemplaire dans sa politique, comme les collectivités locales. Il doit montrer l'exemple. Dans de nombreux cas, il ne l'a pas fait. Je ne vais pas entrer dans les polémiques. Tel n'est pas le sujet. Les collectivités locales doivent obtenir la visibilité complète de la localisation des données, de leur traitement. OVHcloud investit massivement, notamment à travers l'ouverture de deux *data centers* en France qui répondent à la demande de l'État de créer un *cloud* certifié SecNumCloud 100 % français, pour des usines françaises. L'offre est là. Passons maintenant des paroles aux actes.

M. Philippe Latombe, rapporteur. Même si vous ne souhaitez pas entrer dans les polémiques, je me permets de poser des questions sur l'exemplarité de l'État. Nous avons auditionné l'UGAP, et un certain nombre de personnes, qui nous ont expliqué qu'il manquait des solutions françaises ou européennes aussi simples que celles proposées par les Américains, et notamment par Amazon (AWS) ou Microsoft, raison pour laquelle ils avaient choisi ces *clouds*. L'absence d'exemplarité de l'État est-elle liée à une incapacité à trouver des solutions simples ou à construire des solutions avec des acteurs français ? Ou l'idée est-elle de délibérément choisir des solutions toutes faites parce que les compétences n'existent pas en interne, au sein de l'État, ou au sein des entreprises publiques, pour agréger des solutions différentes et en faire un ensemble ? Par exemple, pour le prêt garanti par l'État (PGE), BPI est passé sur AWS, et sur Azure pour la gestion des *mails*, par souci de simplicité. Cette même remarque a été faite et le sera certainement de nouveau lors des auditions sur les données de santé avec le Health Data Hub (HDH) et d'autres acteurs dans une semaine. S'agit-il d'un manque de services liés au *cloud* qui induit ce choix ou d'une absence de volonté ?

Mme Servane Augier. La réponse n'est pas simple. Il y a beaucoup de nuances de gris dans ce débat. Aujourd'hui, toutes les solutions existent en Europe, mais elles sont très atomisées. On compte de nombreux éditeurs différents, de fournisseurs différents. Chez OUTSCALE, nous travaillons sur la mise en place d'un écosystème de confiance qui permette d'agréger, dans une *marketplace*, l'ensemble des solutions. OVH aussi a lancé une *marketplace*. Orange vient d'annoncer le lancement d'une *marketplace*. Il existe un besoin de regrouper les solutions qui, sinon, ne sont pas accessibles de la même manière que sur le

portail AWS. Effectivement, il existe, d'un côté, une solution plus compacte et plus facile d'accès.

Cette solution AWS s'est aussi construite parce que les États-Unis ont adressé des commandes à AWS, qui a pu développer sa R&D, construire ses offres pour répondre aux besoins. La question est de savoir si, en France, on veut se donner les moyens d'aller vers des solutions qui ne sont pas complètement finies, sur lesquelles il faudra travailler un peu, mais qui doivent permettre de renforcer la filière souveraine, ou si la simplicité et la rapidité prévalent. Cela peut être le cas dans certains domaines, mais il faut afficher très clairement que l'on considère un critère de choix autre que la souveraineté.

Cependant, ce choix n'est pas toujours réalisé après avoir effectué un réel examen de ce qui est accessible sur le marché. Des décisions sont prises de manière un peu hâtive, alors qu'il existe des solutions, quasiment aussi rapides, avec des acteurs français. Pendant la crise du Covid, nous avions un programme de solidarité *Act For Life*. Un de nos partenaires a monté en deux jours le site de la réserve civique sur notre *cloud*. De nombreux sites se sont montés très vite sur des *clouds* souverains pendant la période. Pourquoi n'a-t-il pas été possible de monter celui du prêt garanti aux entreprises (PGE) sur un *cloud* français ? Je ne sais pas le dire. Sur le dossier du Health data Hub (HDH), qui est beaucoup plus complexe en termes de services utilisés, le critère de rapidité de mise en œuvre a prévalu. En revanche, sur un site internet, je m'interroge un peu.

Je crois qu'il y a des changements d'état d'esprit à générer. L'idée préconçue que cela sera de toute façon plus facile avec les Américains sur tous les sujets *cloud*, est fausse. Il faut se dire qu'une offre performante existe. Quand le sujet doit être souverain, il faut que l'administration prenne une décision souveraine. Quand cela n'est pas le cas, quand la priorité est l'agilité apportée par des services qui existent pour le moment uniquement chez d'autres fournisseurs, il faut y aller. Ce n'est pas du protectionnisme. Il ne s'agit pas de ralentir l'économie, mais de faire des choix en conscience et de privilégier des solutions souveraines pour les données sensibles.

Mme Karine Picard. Je suis tout à fait d'accord. La force des acteurs américains est d'offrir un tout : l'infrastructure, la plateforme et le SaaS. Cela permet à certaines entreprises de rationaliser leur schéma directeur, de prévoir les intégrations, de faciliter la construction et le *move to cloud* d'un certain nombre de processus. Au départ, les entreprises privées ont fait des choix de *cloud* département par département. La présence de multiples acteurs cloud à l'intérieur d'une entreprise peut engendrer des problématiques de sécurité, de transmission de données, des problèmes légaux. Il existe un besoin de rationaliser, en termes tant de sécurité des données, de souveraineté, que de flux entre les différents départements des entreprises. Peu d'acteurs en Europe peuvent fournir ce type d'offre, cette gamme de services pour les entreprises privées. Il faudra que l'Europe décide d'investir pour créer l'« Airbus de la technologie » avec des sociétés capables de fournir un plus grand nombre de services.

Aujourd'hui, en tant qu'acteur américain, Oracle est positionné sur Cercle 3. Nous faisons partie des éditeurs qui peuvent proposer des solutions de confiance pour un certain nombre de collectivités et d'acteurs publics. Le Cercle 2 est un autre niveau de sensibilité. Que fera le Gouvernement au niveau du Cercle 2 ? Se rapprochera-t-il de Gaia-X ? Quels seront les critères établis ? Étant donné la sensibilité des données, nous ne nous positionnerons jamais, en tant qu'acteur américain, sur Cercle 1. En tant qu'acteur extraterritorial (hors France ou hors Europe), il est important de se positionner sur les niveaux de sensibilité qui sont appropriés par rapport aux demandes des gouvernements.

Lorsque le niveau de sensibilité des données est moindre, il est nécessaire de regarder quelle est la meilleure solution, pour le département, à l'instant T, ce qui est le plus rapide à mettre en place. Vous le disiez, M. Michel Paulin, la transparence et la compétitivité sont très importantes. L'État doit avoir le choix de faire jouer la concurrence. Il ne doit pas se retrouver pieds et mains liés à un ou deux vendeurs, peut-être souverains, mais qui ne feront pas jouer la concurrence et dont les prix ne seront pas en phase avec ce que l'État peut investir et avec les réductions de coût qui seront nécessaires dans les années à venir. Comment les fournisseurs souverains permettent-ils de garantir cette compétitivité des prix pour l'État, en termes d'investissement ?

M. Michel Paulin. Je ne suis pas tout à fait d'accord. À ma connaissance, avec OUTSCALE, nous sommes largement moins chers que tous les *hyperscalers*. Vous pouvez regarder tous les *benchmarks* publics : nous sommes beaucoup moins chers. La notion de compétitivité en termes des prix/performance n'est pas un argument opposable aujourd'hui. C'est plutôt l'inverse. Le Cigref se plaint de la position dominante de certains des acteurs qui profitent de leur position dominante pour imposer leur *cloud*. Les acteurs de SaaS en particulier imposent le stade en dessous pour pouvoir justifier de l'évolution technologique et l'augmentation des prix. Aujourd'hui, un certain nombre de clients se retrouvent, avec des *hyperscalers*, dans des situations où leurs coûts augmentent fortement. De plus, ces *clouds* sont fermés, sans *API* et ne sont ni transparents ni réversibles. Nous sommes dans une double problématique. De notre côté, nous travaillons pour fournir des solutions souveraines, avec des *API* ouvertes, de l'*open source*, avec des prix largement plus compétitifs que la majorité des *hyperscalers*. Nous nous sommes toujours engagés dans la filière à maintenir nos prix à un niveau compétitif, quelles que soient les contraintes posées par l'État.

Le deuxième point que je souhaitais évoquer est cette notion de simplicité. Nous n'avons pas la prétention de dire que l'on pourra couvrir tous les besoins de tous les acteurs. D'ailleurs, quel opérateur peut le prétendre ? Même AWS ne dispose pas de solution collaborative, qui est pourtant un besoin extrêmement important. Cela prouve que le leader mondial n'est pas en mesure de proposer l'ensemble des solutions. En revanche, il est vrai que les *hyperscalers* ont une gamme plus large. Ils sont partis plus tôt, ils ont été financés par leur pays. Ils ont bénéficié d'un soutien très puissant de leur écosystème régional. L'Europe n'a pas pu mettre en œuvre un tel soutien. Cette simplicité présente un certain nombre d'inconvénients. La solution est bien souvent monolithique, horizontalement ou verticalement. En effet, à l'horizontale, vous n'avez pas le choix sur les sous-ensembles, vous êtes obligés de tout prendre. À la verticale, il est obligatoire de prendre l'ensemble du *cloud*. Le *multi-cloud* est impossible. Aujourd'hui, beaucoup de grands comptes ont l'impression d'être pris dans un étau dans lequel ils sont enfermés d'un point de vue contractuel. Le Cigref a désigné les lauréats des mauvaises pratiques concurrentielles dans le domaine de la technologie de l'information (IT). Ces solutions sont apparemment plus simples, mais il faut en comprendre les conséquences.

Nous souhaitons que l'écosystème d'OVHcloud, avec des partenaires (qu'ils soient des éditeurs américains ou européens), puisse fournir l'essentiel des besoins des entreprises dans le domaine du IaaS et du PaaS. Aujourd'hui, oui, nous pensons que nous pouvons répondre à l'essentiel des besoins. Notre croissance le prouve. Nous ne sommes pas un acteur en difficulté. Nous sommes profitables, nous investissons, nous recrutons. Cela montre que nos solutions répondent à une grande partie des besoins des petites et grandes entreprises aujourd'hui. Servane Augier le prouve également à travers l'écosystème qu'elle a monté. Certains sont d'ailleurs communs.

Nous sommes dans des solutions complètement différentes de la philosophie des *hyperscalers*. Il s'agit de solutions ouvertes, réversibles, *multi-cloud, hybrid-cloud*. Le client garde la maîtrise de la solution. Ces solutions sont peut-être un peu plus complexes à mettre en œuvre, nous en convenons. C'est pour cette raison que nous travaillons sur des labels, sur des intégrations, sur des *marketplaces* intégrées afin de faciliter, pour l'utilisateur final, l'usage de ces solutions. Nous avons annoncé des intégrations de solutions. Paradoxalement, nous avons signé un accord avec *Google Cloud,* dans lequel nous avons garanti la souveraineté des données de manière très stricte (le *disconnect*) et nous intégrons des technologies dans un *control panel* qui fait que, pour le client, l'utilisation de ces technologies sera extrêmement simple. Nous fournissons beaucoup d'efforts pour simplifier en gardant, contrairement à certains acteurs, les *API* ouvertes à la fois à l'horizontale et à la verticale.

Le fait de dire que les acteurs ne sont pas capables de répondre à l'ensemble des demandes est une facilité intellectuelle. Bien souvent d'ailleurs, il n'y a pas d'appel d'offres. L'effort d'analyse n'a pas été fait. Aujourd'hui, sur un sujet comme le web, sur lequel nous sommes numéro 1 français, nous avons des choses à faire valoir. Nous ne sommes pas numéro 1 par hasard. Nous sommes un des hébergeurs les plus puissants sur les grands et les petits sites. Sur ce sujet, nos arguments sont nombreux et prouvent que nous possédons les solutions. Faut-il encore être consultés et pouvoir répondre de manière équitable et sans exclusivité. Il faut qu'il y ait de la concurrence, de l'innovation. C'est important. Vous connaissez nos positions publiques sur un certain nombre de sujets : nous attendons l'appel d'offres et nous y répondrons.

M. Philippe Latombe, rapporteur. Vous avez évoqué la transparence et la réversibilité. Les *providers* de *cloud* sont-ils nombreux à ne pas proposer la réversibilité ou à mettre des freins à la réversibilité ?

M. Michel Paulin. C'est sûr. Ce n'est pas moi qui le dis, c'est *Gartner*.

M. le président Philippe Latombe. Ces freins sont-ils financiers ou technologiques ?

M. Michel Paulin. Ils sont de trois ordres. Le premier est technique. C'est par exemple le fait de ne pas avoir d'*API* documentés pour être capable de faire de la réversibilité, d'avoir des systèmes monolithiques dans lesquels vous mettez plein de modules liés par essence, où il est difficile de délier le stockage du *compute*, délier l'IaaS du SaaS ou du PaaS. Par exemple, il n'est pas possible de ne pas avoir Azure sur Office 365.

Le deuxième aspect est financier. Cela a été mentionné par *Gartner*, par IDC, par Forester. Comment les données sont-elles facturées quand on sort du système (l'*in and out* dans la bande passante) ? Certains acteurs font payer très cher la sortie des données de leur environnement. Notre politique tarifaire est que le prix de la bande passante dans les *data centers* en entrée ou en sortie est compris dans le forfait. C'est pour cette raison que nous sommes massivement moins chers que les autres.

Enfin, le troisième sujet est légal. Si vous voulez avoir accès à un certain nombre de niveaux de licences, vous êtes obligés de choisir un *cloud* en dessous. Je ne suis pas le seul à le dire. La Chambre des Représentants américaine a estimé qu'un certain nombre de pratiques commerciales de certains acteurs aux États-Unis mettaient en danger la concurrence et l'innovation.

La réversibilité est un des principes fondamentaux de Gaia-X. Nous sommes très heureux de voir que, malgré le scepticisme de départ, de nombreux acteurs se sont engagés sur ce principe. À nous maintenant, en tant que membres du conseil d'administration de Gaia-X, d'être vigilants pour que les critères déterminants du label Gaia-X soient scrupuleusement respectés. Il faut que personne ne se réfère à Gaia-X sans respecter ces critères. Les critères les plus importants sont la réversibilité réelle, la transparence complète de bout en bout, horizontale et verticale, le fait de favoriser l'interopérabilité. Le *multi-cloud* est la solution pour les clients. Il garantit une compétition saine. Les systèmes de *lock up* juridique, tarifaire ou technique doivent être évités. Nous poussons beaucoup dans le domaine du *public cloud* pour avoir un acteur majeur dans l'*open source*. Nous continuons à investir massivement. Nous venons de réaliser deux acquisitions en nous engageant à redistribuer dans le domaine de l'*open source* les technologies que nous développons pour pouvoir proposer des distributions accessibles à tous avec des *API* documentés qui garantissent les principes fondateurs de Gaia-X.

M. Philippe Latombe, rapporteur. Souhaitez-vous que le législateur, français ou européen, légifère sur les ventes liées (*cloud* + licence), comme cela a pu arriver dans d'autres domaines ? Faut-il légiférer sur les *vouchers* que proposent certains *clouds* au début de la création d'une start-up pour les faire travailler directement sur leur environnement ? Ce point a été remonté il y a quinze jours. Cette pratique commerciale des *vouchers* biaise la concurrence. Souhaitez-vous que le législateur, français ou européen, légifère sur ce sujet ?

Mme Servane Augier. La législation à l'échelle européenne sur les ventes liées me paraît absolument indispensable. Le rôle du droit de la concurrence est de s'assurer que la concurrence reste saine. Sur des domaines aussi monopolistiques qu'Office 365 avec Azure, il est indispensable que l'Europe s'en saisisse et légifère.

S'agissant des *vouchers* et des *welcome kits*, je ne pense pas qu'il faille légiférer pour les empêcher. Toutefois, nous remarquons qu'un certain nombre de start-up viennent chez nous dans un deuxième temps. Elles utilisent ce *welcome kit*. On ne va pas leur reprocher d'utiliser ce qu'on met à leur disposition, mais elles se rendent vite compte du risque important de perte de maîtrise. En effet, quand on utilise la panoplie des services de nos concurrents, on ne maîtrise plus l'infrastructure technique et le SI qu'on est en train de déployer. Les start-up viennent ensuite chez nous parce que nos *API* sont compatibles avec ceux d'*AWS* en l'occurrence. La migration est très facile et elles trouvent chez nous cette interopérabilité et cette capacité à rester en maîtrise complète de leur système d'information.

Lorsque l'on finance une start-up, on devrait s'assurer qu'on la finance en lui mettant à disposition des solutions souveraines. Il convient de travailler pour faire en sorte que les financements embarquent un *welcome kit* souverain. Si l'on finance, autant le faire en fournissant un service qui fera également du bien à l'État.

M. Michel Paulin. Les ventes liées et les ventes forcées sont du domaine de la concurrence. Je ne sais pas s'il faut légiférer, mais ces pratiques devraient être dénoncées. Elles ne sont pas saines. La législation concerne plutôt la protection des données sensibles. La législation devrait imposer la transparence pour qu'il y ait une liberté de choix de bout en bout et imposer des critères de réversibilité. Il faut éviter de lier systématiquement un éditeur de logiciel SaaS avec un *cloud* imposé dans lequel vous n'avez pas le choix. La législation semble nécessaire puisque certains acteurs ne le respectent pas.

Je ne sais pas s'il faut légiférer pour empêcher les *vouchers* pour les start-up. Certaines pratiques incluent des notions d'exclusivité dans le temps, ce qui entraîne comme l'a dit Gilles Babinet, le « syndrome de l'héroïne ». Une fois qu'une start-up a commencé à mettre le doigt dedans et qu'elle est liée à un fournisseur par un contrat d'exclusivité pour quatre ou cinq ans, il est très difficile de revenir. Le coût pour en sortir est élevé. Nous voyons effectivement un certain nombre de start-up revenir en disant que les notions d'adhérence et de *lock up* sont dangereuses pour elles. Elles veulent des stratégies *multi-cloud* et reviennent vers des acteurs comme OUTSCALE ou nous-mêmes. Cette notion d'exclusivité à long terme, associée à ce *voucher,* n'est pas saine en matière de compétitivité. Même si au début, ce dispositif donne des capacités de développement, il n'est pas pérenne.

Il est nécessaire de clarifier ces règles du jeu. L'État doit participer à cette pédagogie. Les élus doivent s'intéresser à ces sujets. Il faut comprendre que ces sujets sont complexes : l'IaaS, le PaaS, le SaaS… Nous sommes assez mauvais dans la pédagogie et d'autres ne font pas l'effort. Nous devons le faire auprès des citoyens, des représentants de la nation. L'État doit participer à la clarification pour donner tous les éléments. Mon message n'est pas de dire que nous voulons de l'exclusivité, du protectionnisme. Nous voulons au contraire un *cloud* ouvert, réversible, transparent, qui donnera les garanties légales, techniques et financières à l'ensemble des acteurs pour pouvoir protéger leurs données dans le cadre européen, en dehors des solutions extraterritoriales. Il ne s'agit pas de choisir un acteur dans chaque pays qui deviendra l'acteur référent et qui aura le monopole. Si aujourd'hui les hommes politiques ne décident pas de protéger, il y aura *de facto* des monopoles extrêmement puissants, avec des acteurs qui sont aidés. Dans certains domaines, l'informatique ou le digital, il n'y a plus qu'un ou deux acteurs au niveau mondial. Prenez le *search* ou les grands domaines digitaux autour des réseaux sociaux.

Le *cloud* doit rester un secteur concurrentiel et ouvert et qui respecte les valeurs européennes de protection des données. Le cadre juridique que nous demandons est exactement celui-là. Le risque est de voir une prédominance d'un certain nombre d'acteurs qui vont préempter un marché extrêmement intéressant, d'un point de vue financier, le fameux « pétrole du 21ème siècle ». Mais il y a des enjeux éthiques. Où sont les données de santé ? Comment sont-elles traitées ? Qui a le droit d'en faire quoi ? La régulation de ces données doit être à l'agenda des représentants européens et français. C'est également un enjeu géopolitique. Nous l'avons vu pendant la crise. Comment s'effectueront les allocations des ressources digitales pendant des crises de cette nature ? C'est devenu une question géopolitique. Le fait que la présidence américaine ait décidé de supprimer TikTok prouve l'existence de ces enjeux.

Le Cigref a clairement dit que les grandes entreprises étaient inquiètes des décisions d'arbitrage qui seraient prises sur les composants, les logiciels, les bandes passantes, sur les sujets d'allocations des ressources, dans des situations de pénurie ou de crise. Il est important que l'Europe se saisisse de ce sujet et garantisse une ouverture et une compétitivité de l'ensemble du marché, plutôt que de le refermer avec quelques acteurs, et fasse en sorte qu'il y ait une indépendance, une souveraineté, une possibilité de choisir. Sur ces sujets, nous militons avec OUTSCALE ou avec des acteurs en Allemagne, en Italie, en Espagne, avec lesquels nous avons monté des partenariats.

Mme Karine Picard. Nous militons pour les mêmes choses. Nous militons pour la transparence depuis toujours. Pour cette raison, nous n'émergeons nos solutions que sur des *clouds* sur lesquels nous pouvons garantir l'intégralité, la sécurité, la localisation des données et qui les opère. Je suis d'accord avec vous. Nous nous battons contre d'autres vendeurs qui

hébergent chez Google, Amazon, et autres, sans avoir la garantie de la chaîne complète de la sécurité de la donnée. Leurs clients ne peuvent pas choisir avec qui ils veulent travailler. L'ouverture, la transparence, la réversibilité sont des sujets sur lesquels nous travaillons, depuis toujours, en tant qu'opérateur de cloud. C'est de cette façon que nous nous sommes différenciés d'Amazon, Google, etc. De plus, nous travaillons depuis toujours sur du *BtoB*. Les données de nos clients n'appartiennent qu'à nos clients. En aucun cas, nous ne ferons du *business* sur la donnée. Il y a une différence entre les *providers* de *cloud* qui font du *BtoC* et ceux qui font du *BtoB*. C'est aussi un élément de pédagogie envers les citoyens, qui ne comprennent pas forcément toutes ces subtilités.

M. Philippe Latombe, rapporteur. D'un point de vue juridique, *Schrems* II a constitué une vraie rupture. Quelle analyse en faites-vous ? Quelles sont les conséquences de *Schrems* II qui nécessitent des clarifications ? Comment peut-on se prémunir de l'extraterritorialité, notamment américaine ? Y a-t-il des mesures juridiques à prendre pour donner un cadre plus clair, puisque SecNumCloud ne garantit pas l'absence d'extraterritorialité ? Que faut-il faire juridiquement pour clarifier les choses ?

Mme Servane Augier. Dans les discussions à la direction générale des entreprises (DGE), avec le Comité stratégique de filière, nous avons travaillé sur l'éventuel renforcement de la loi de blocage qui viendrait en contrepoids du *Cloud Act*, et qui viendrait flécher la donnée sensible vers des *clouds* de confiance. Nous appelons à la création d'un label permettant de clarifier le paysage et d'adresser des messages clairs aux futurs clients. La souveraineté est la capacité à choisir. Cependant, pour choisir de manière éclairée, il est utile d'avoir des panneaux explicatifs. Les acteurs ne peuvent pas dresser eux-mêmes les panneaux, au risque d'être juges et parties. Ce que nous décrétons est moins fort que ce que quelqu'un peut nous attribuer comme mérite. C'est pourquoi nous sommes très enclins à passer des certifications. Nous pensons que la confiance se prouve. Je souhaite que l'État mette en place un système permettant de savoir quels labels garantissent le respect des critères de non-soumission à des réglementations extra-européennes.

M. Michel Paulin. Je suis tout à fait d'accord. Je pense que l'on commence tout juste à s'apercevoir des conséquences de *Schrems* II. Ses implications sont extrêmement fortes. *Schrems* II interdit l'export de toutes données et de métadonnées en dehors de la Communauté européenne. Cela met, de manière indirecte, beaucoup de solutions dans l'illégalité complète.

Avec la filière, nous sommes très à l'aise : avec nous, le client choisit la localisation de ses données et nous garantissons l'absence de transferts de données et de métadonnées. De plus, nous n'accédons pas aux données du client, puisqu'aucune des données ne transite. Nous sommes confiants sur le fait d'être totalement conformes à l'ensemble des recommandations *Schrems* II.

Aujourd'hui, certains clients ont des logiciels avec la paie de leurs salariés qui sont hébergés aux États-Unis, avec des métadonnées qui circulent aux États-Unis. Il s'agit parfois de leur base client, avec les noms, les emails, les numéros de téléphone. Et même si ces données sont hébergées dans un *data center* quelque part en Europe, il arrive souvent qu'elles transitent. Il ne serait pas étonnant que certains acteurs lancent des *class actions* visant les acteurs qui ne seront pas capables de respecter *Schrems* II. Des directeurs juridiques d'entreprise viennent nous voir en nous demandant s'ils sont exposés. En général, la réponse est : *« Oui, vous êtes exposés. Il existe un vrai enjeu pour la protection des données de vos*

salariés, de vos clients ». Ils découvrent avec surprise qu'ils sont très exposés, car ils n'avaient pas été très attentifs lors des appels d'offres sur ces sujets.

Schrems II est en train de radicalement changer les modèles. Cette exigence sera de plus en plus présente. C'est pourquoi les labels sont très importants. Il faut passer de labels uniquement techniques à des labels qui permettront de gérer le problème de la sécurité et le problème légal. Certains *hyperscalers* disent qu'il suffit d'encrypter les données. Tout le monde sait que le chiffrement peut se casser. Certains pays exigent que toutes les clés utilisées par les fournisseurs soient hébergées sur place. Cela prouve bien que le sujet n'est pas uniquement technique. Il doit être légal. Je souscris tout à fait à la recommandation de Servane Augier sur le fait que la labellisation HDS doit inclure un certain nombre de garanties légales sur le stockage et l'utilisation des données. Il faut garantir qu'elle est conforme à *Schrems* II. Le législateur et la force publique doivent intervenir. Ils doivent être capables de garantir la légalité dans le cadre de *Schrems* II.

Mme Karine Picard. Du fait de l'endroit où nous localisons nos données et de l'absence de transfert de données entre les *data centers* à l'extérieur de l'Europe, nous respectons *Schrems* II. Les investissements massifs que nous effectuons en Europe sur les *data centers* sont aussi en précaution de la régularisation. Contractuellement, nous devons protéger nos clients et respecter *Schrems* II. Plusieurs acteurs vont se retrouver dans l'illégalité aujourd'hui. Les investissements massifs en Europe sont la garantie que nous respectons les lois.

M. Michel Paulin. Je me permets de « challenger » cette affirmation. L'une des implications de *Schrems* II est que le fournisseur de *cloud* est exclusivement soumis à la juridiction de l'Union européenne, à l'article 48 du RGPD. Or le *Cloud Act*, dans la juridiction, impose aux acteurs américains de fournir des données sur injonction. C'est cadré, mais selon moi, il existe un enjeu. Dès qu'un acteur est soumis au *Cloud Act*, il est exposé à ne pas être conforme à *Schrems* II.

Mme Servane Augier. C'est mon point de vue également. Au-delà des efforts fournis par Oracle, dans la mesure où il n'y a pas d'accord entre les États-Unis et la France ou l'Europe, il existe une incompatibilité. Vous êtes dans un *corner*. Pour les acteurs américains présents en France et en Europe, le RGPD, *Schrems* II et le *Cloud Act* donnent des injonctions contradictoires.

Mme Karine Picard. Il faudra faire appel au pragmatisme économique, si on ne veut pas que toutes les entreprises européennes se retrouvent dans l'illégalité.

Mme Servane Augier. Bien sûr. J'évoquais l'aspect juridique.

M. Philippe Latombe, rapporteur. *Schrems* II a invalidé le transfert, mais maintient les clauses contractuelles. Les entreprises comprennent-elles les implications ? Sont-elles en capacité de négocier ces points ? Faut-il intervenir, et, si oui, comment, sur les clauses contractuelles ?

Mme Servane Augier. Je vois se multiplier les webinaires à destination des clients pour leur parler des conséquences de *Schrems* II, de ces clauses contractuelles. Il existe une difficulté de compréhension. La première intervention serait de créer un *vademecum* à l'intention des entreprises françaises sur ce qui fonctionne, sur les aspects où la prudence est de mise, sur les contrats à revisiter. Aujourd'hui, tout le monde improvise. En fonction de la

sagacité des *data protection officers* dans les entreprises, certains sujets seront soulevés ou non. Un petit guide à l'attention des entreprises sur les points de vigilance serait pertinent. Nous entendons parler d'amendes qui peuvent être considérables. Il ne faut pas punir l'économie française avec ces difficultés contractuelles.

M. Michel Paulin. Tout à fait. Il n'existe pas de jurisprudence aujourd'hui. Il y a le droit et l'utilisation du droit. Tout ce qui permettra d'éclairer les décideurs sera intéressant. Je pense que ce sujet dépasse les clients. Notre sondage est très clair. Les citoyens demandent de la transparence sur les sujets de santé. Il faut clarifier la législation en ces domaines.

Le *cloud* de confiance tel que nous le concevons est une des solutions pour la souveraineté, mais aussi pour répondre aux exigences éthiques. Il convient de continuer la pédagogie. Ces secteurs sont parfois un peu complexes. Les entreprises ne sont pas forcément des spécialistes. Il faut éclairer, faire de la pédagogie, ouvrir les boîtes noires lorsque cela est nécessaire. Les clients doivent utiliser l'arrêt *Schrems* II pour retrouver une capacité de choix, de liberté. Le *cloud* de confiance facilite l'innovation et la compétition. Ce n'est pas un *cloud* fermé. L'argument qui consiste à dire que ce que nous proposons bloquera l'économie est faux. Nous demandons une régulation équitable, qui permette d'éviter que certains acteurs préemptent les marchés. De plus, notre *cloud* garantit aux citoyens une protection des données qui est légitime, mais qui est minoritaire dans le monde. Le RGPD est une pratique européenne, et non mondiale. Dans certains pays, on observe une mutualisation forcenée de la donnée pour imposer, contrôler, voire réprimer.

Mme Karine Picard. Il est nécessaire de clarifier *Schrems* II, car les éditeurs ou les entreprises n'en comprennent pas les conséquences. Nous sommes conformes au RGPD, qui est clair, mais il faudra apporter de la clarté juridique sur *Schrems* II pour que nous puissions nous positionner. Le flou pour les entreprises, en période de Covid, n'est pas opportun. Elles doivent investir dix fois plus rapidement pour s'adapter et faire face à la crise. Le flou autour des contrats qu'elles auront le droit de conclure et des risques qui existent retardera les entreprises dans leur choix et donc dans leur transformation digitale, ce qui n'est dans l'intérêt de personne. Cette clarté est extrêmement importante. Il faut laisser la possibilité aux entreprises de choisir les solutions les plus sûres et les plus pertinentes par rapport à leur métier et à leurs besoins. La clarté est indispensable, étant donné la situation actuelle. Les entreprises n'ont pas arrêté leurs investissements digitaux. Il convient de les accompagner au mieux dans la clarté.

M. Philippe Latombe, rapporteur. Je vous pose la question d'un collègue qui souhaite revenir sur la formation des acteurs. Comment pouvons-nous former les acheteurs pour combattre cette forme d'autocensure des directions des systèmes d'information (DSI) quant à l'achat de solutions sortant des habitudes ? Il a été indiqué dans une des auditions précédentes que les acheteurs publics sont plutôt des spécialistes juridiques, des spécialistes du contentieux des marchés publics que des acheteurs de solutions, avec une fibre technologique. Auriez-vous des propositions pour faire en sorte que les marchés soient mieux définis et que les acheteurs soient plus informés des solutions existantes ?

Mme Servane Augier. Il serait important que la doctrine de l'État soit plus claire et qu'elle soit descendue dans les administrations déconcentrées et dans les collectivités territoriales. L'UGAP a fait un travail formidable pour mettre en place un marché de référencement qui apporte des outils. Parmi ces derniers, tous les *cloud providers* sont référencés, les *cloud providers* français, les *cloud providers* américains. Il n'existe pas de mode d'emploi pour l'accompagner, de doctrine de l'État disant : *« nous vous donnons des*

outils, parce que vous avez besoin de choix, d'agilité dans votre transformation cloud *en région. Nous vous recommandons de faire tel ou tel choix en fonction de tel ou tel critère »*. Il faut clarifier, prendre parti et dire : *« Nous, en tant qu'État, recommandons que les données de santé locales, que les données financières, que les données des citoyens restent sur des* clouds *de confiance. Cela signifie de faire appel à tel ou tel fournisseur pour tel usage. Vous pouvez choisir plus largement pour telle autre typologie d'usage. »*

En parallèle, les acteurs s'engagent, notamment à travers Gaia-X, à favoriser l'interopérabilité et le *multi-cloud*. Nous ne souhaitons pénaliser ni bloquer personne. Cependant, dans certains domaines, il est essentiel de respecter ces sujets de souveraineté. Pour ce faire, il est important que les acteurs du *cloud* soient interopérables. En effet, il faut qu'une entreprise puisse choisir un *cloud* dans un cas et un *cloud* différent dans un autre cas, sans que cela ne soit compliqué. Il convient que l'État s'exprime clairement sur la doctrine et donne des consignes. Je suis en train de prononcer des mots tabous, mais il est regrettable que les marchés arrivent jusqu'aux acteurs locaux sans mode d'emploi. Il est étonnant de référencer pour le *cloud* de l'État tous les acteurs américains pendant que M. Bruno Lemaire évoque la nécessité de créer une offre souveraine. Cela génère des interrogations. Il faut expliquer ce que l'État a voulu faire en référençant tous les acteurs, tout en poussant les offres souveraines. Il est utile de clarifier les consignes.

Mme Karine Picard. Je suis tout à fait d'accord avec vous. Nous faisons partie de Cercle 3. Nous garantissons un certain nombre d'éléments, en termes de réversibilité, d'ouverture, de localisation des *data centers*, de sécurité, de points techniques. Pourtant, nous nous retrouvons en compétition avec des acteurs américains qui ne respectent pas ces éléments. Nous sommes assimilés à eux. Les raccourcis effectués, de par ce manque de clarté, pénalisent à la fois les acteurs souverains français, mais aussi les acteurs étrangers américains qui respectent ces règles à 100% et qui sont entrés dans le marché Cercle 3. Plus personne ne comprend rien. Cet élément de clarté est extrêmement important nous nous aussi. Il arrive que nous soyons emmenés sur des appels d'offres pour, au final, nous rendre compte que nous ne pouvons pas le remporter en raison de notre nationalité. Les vendeurs ont besoin de clarté pour savoir quels types d'appels d'offres sont ouverts ou non.

M. Michel Paulin. Je suis à 100 % d'accord avec vous. Il faut faire preuve de pédagogie auprès des acheteurs, les former. Il est vraiment très compliqué de comprendre les implications de *Schrems* II. Il faut former l'ensemble de l'écosystème. Il est nécessaire que l'UGAP aille plus loin dans la transparence des critères de choix. La localisation des données doit être un critère, indépendamment de la nationalité de l'opérateur. Le fait qu'un certain nombre des données de santé soient à Amsterdam n'est pas forcément un problème, mais nous devons le savoir. Il faut qu'ensuite les décideurs prennent les bonnes dispositions.

De la même façon, les critères de certification technique ou légale doivent être des indicateurs accessibles à l'acheteur. Il est utile d'avoir des recommandations par rapport à un certain nombre de sujets. Il est clair qu'il n'est pas toujours indispensable que les données ne transitent pas. Certaines ne sont pas considérées comme sensibles. En revanche, sur certaines données, il est impératif, même dans le cadre du Cercle 3, que le discriminant soit fait sur des acteurs complètement ouverts et transparents sur certains principes. Il faut cette clarté de bout en bout. Cela doit être un critère de choix. Cela ne peut pas être uniquement *nice to have*. Cela doit être une obligation. L'État et les marchés publics doivent donner des règles, et donner les moyens aux acheteurs de prendre des décisions. Sinon, ce qui prévaudra sera, soit une nationalité unique des acteurs, soit un obscurantisme des conditions du process, qui entraînera

la réflexion : *« C'est plus simple avec l'acteur qui remporte tout »*, *first takes all* et c'est terminé. Ce sera un monopole de fait.

Il faut faire de la pédagogie et imposer. Pour l'UGAP par exemple, les appels d'offres publics doivent être très clairs sur les conditions d'attribution sur l'ensemble de la chaîne. Certains appels d'offres intégrateurs produisent des sites web. Il convient de savoir où sont hébergés ces sites web, comment, où sont les données, comment elles transitent. Ces informations doivent apparaître de manière claire, pour que le cahier des charges donne de la visibilité. Une fois que tout cela est décrit et certifié, chacun décide en toute connaissance de cause. En revanche, sur un certain nombre de données sensibles, considérées par l'État comme stratégiques et devant être gérées par des opérateurs souverains, il convient de voter une loi. Les données des OIV, des grands acteurs doivent rester dans des conditions de souveraineté totale.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous évoquer des sujets que nous n'avons pas abordés ?

Mme Servane Augier. Pour encourager cette filière souveraine, il conviendrait de traiter le sujet avec les écoles. Les ingénieurs qui arrivent sur le marché veulent travailler avec ce qu'ils ont utilisé à l'école. Il est important que les solutions souveraines soient accessibles et disponibles dans les écoles. C'est un axe de travail. L'État a mis en place des plans d'accélération, des appels à manifestation d'intérêt (AMI). Il existe une vraie motivation pour que la filière se développe. Par ailleurs, il conviendrait de traiter des sujets de fiscalité. Le FCTVA est une première bonne nouvelle pour les collectivités territoriales qui pourront avoir le même niveau de TVA qu'elles soient en OPEX ou en CAPEX sur ces sujets. Des dispositifs de fiscalité pourraient être mis en place, avec des politiques de suramortissements, pour encourager les investissements des sociétés qui paient leurs impôts en France.

M. Philippe Latombe, rapporteur. Nous avons décidé d'ouvrir une séquence sur la formation fin mars/début avril. Le sujet de la formation primaire jusqu'aux grandes écoles sera abordé. Nous sommes preneurs de vos propositions sur les différentes thématiques que nous évoquerons au sein de la mission. N'hésitez pas à continuer à contribuer par des écrits que nous annexerons au rapport.

Mme Karine Picard. En tant qu'acteurs américains, notre puissance d'investissements nous a permis, pendant la crise, de mettre à disposition d'un certain nombre de gouvernements des solutions pour « monitorer » ce qui se passait sur les traitements du Covid, sur les vaccins. Ces solutions ont été proposées aux gouvernements européens. Du fait de ce manque de clarté sur les données de santé, le Gouvernement français ne pouvait pas prendre ce type de solutions. Cette absence de clarté a empêché certains gouvernements de bénéficier d'innovations qui pouvaient aider à améliorer les process, le pilotage des données en période de crise. Cette clarté est indispensable, car nous apportons le niveau de sécurité nécessaire à un cloud de confiance. Nous faisons les investissements nécessaires.

Vous parlez d'aider les entreprises françaises et européennes. Le sujet du *cloud* est un sujet d'investissement en continu. Cela nécessite d'avoir les fonds pour répondre à la créativité des attaques aujourd'hui. Cette notion d'investissement est essentielle. Aujourd'hui, nous essayons de montrer à nos clients que la souveraineté et la sécurité sont indissociables, même pour un acteur américain. La notion d'investissement n'est pas qu'un élément légal. Derrière la capacité à sécuriser les données, les besoins d'investissement sont gigantesques. Il

faut que l'État et l'Europe prennent conscience des investissements nécessaires pour offrir la meilleure sécurité du *cloud* aux citoyens et aux entreprises.

Mme Servane Augier. Nous n'avons pas abordé les sujets de cyber sécurité. Il est très intéressant que vous receviez Hexatrust jeudi prochain.

M. Michel Paulin. Des actions concrètes peuvent être mises en place, par l'exécutif ou le législateur, autour de la souveraineté des données, pour rendre le process plus transparent. L'idée est d'éditer des règles qui aideront, à la fois, les acheteurs et les citoyens, pour garantir la souveraineté des données sensibles. La notion de régulation et le fait d'ériger des lois ne sont pas tabous, même si, bien souvent, on oppose loi et business. Toutes les autres régions le font. Nous savons que les États-Unis ont régulé un certain nombre de leurs données sensibles. Et je ne parle pas des Chinois qui ne travaillent qu'avec des acteurs 100 % chinois. Des acteurs mettent en place des mécanismes pour protéger leurs données et leur industrie.

La notion d'investissement est importante. Le marché européen est le premier marché mondial. Il existe des opérateurs européens qui ont la capacité de répondre dans de nombreux domaines. Il faut choisir ses batailles. Pour certaines d'entre elles, il vaut mieux faire des alliances ouvertes, conformes aux règles de l'Europe sur la protection des données. Pour d'autres domaines – la sécurité, l'intelligence artificielle, le *big data* – l'Europe a des solutions extrêmement innovantes. Il faut les aider, comme le font les autres régions, qui sont capables de créer des écosystèmes aux États-Unis, en Inde, en Russie, au Japon, en Corée, en Chine, pour faire émerger les acteurs qui auront la taille suffisante pour les investissements nécessaires. Il existe un écosystème à travers la filière française et européenne. L'État doit aider par le cadre législatif, mais aussi, comme dans les autres régions, par la commande publique et par les investissements, à faire émerger ses champions.

La séance est levée à 12 heures 40.

Membres présents ou excusés

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

Réunion du mardi 9 février 2021 à 11 heures

Présent. - M. Philippe Latombe

Excusée. – Mme Frédérique Dumas