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
18 mars 2021
Séance de 14 heures

Compte rendu n° 45

SESSION ORDINAIRE DE **2020-2021**

Présidence de M. Philippe Latombe, *rapporteur*

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de MM. Jean-Claude Laroche, vice-président, et Henri d'Agrain, délégué général, du Club informatique des grandes entreprises françaises (Cigref)

La séance est ouverte à 14 heures 20.

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, président et rapporteur. Nous auditionnons M. Jean-Claude Laroche, vice-président du Club informatique des grandes entreprises françaises (Cigref) et président du cercle cybersécurité de ce dernier, ainsi que directeur des systèmes d'information (DSI) du groupe Enedis. M. Henri d'Agrain, délégué général du Cigref, appartient en outre à la Commission supérieure du numérique et des postes (CSNP), à titre de personnalité qualifiée.

Le Cigref est une association fondée en 1970 par Pierre Lhermitte, dans le but de promouvoir les échanges entre les grandes entreprises et les administrations publiques sur les enjeux du numérique. Il regroupe 150 membres, privés et publics. Il porte, avec d'autres acteurs, le French GAIA-X Hub, dont la première réunion plénière s'est déroulée le 22 janvier dernier.

Je souhaite vous poser trois questions et, pour commencer, une question rituelle de la mission : que recouvre la notion de souveraineté numérique ? Depuis la crise sanitaire, ce sujet fait l'objet d'une attention croissante de la part des pouvoirs publics. Je souhaiterais donc savoir comment le Cigref aborde cette question.

Vous êtes particulièrement mobilisés pour que la France, et surtout l'Europe, sortent de l'« excès d'angélisme » dont elles ont pu faire preuve par le passé, pour citer votre président, M. Bernard Duverneuil. Je suis intéressé par les priorités du Cigref et votre analyse des différentes initiatives européennes dans ce domaine.

Dans un deuxième temps, je souhaite échanger avec vous sur la numérisation des entreprises. Sous l'angle de la demande, quelles sont les attentes et les difficultés des entreprises françaises, mais aussi européennes ? L'offre est-elle en adéquation ? Nous parlerons notamment du *cloud* et de l'initiative GAIA-X. Nous sommes ouverts à toute proposition permettant d'encourager le recours à des solutions et à des matériels souverains.

Enfin, j'aimerais aborder l'enjeu de la cybersécurité sur lequel le Cigref est en veille constante. L'actualité est marquée par la révélation régulière de cyberattaques et la crise sanitaire a donné une visibilité nouvelle à cette menace qui devient de plus en plus sophistiquée. Je voudrais connaître vos attentes vis-à-vis des fournisseurs de service, mais aussi des pouvoirs publics. Nous avons pleinement conscience que la question cyber est un enjeu de confiance, de sécurité et de coût pour les entreprises, en particulier lorsqu'elles sont victimes d'attaques.

Je souhaite également vous entendre sur le volet formation aux savoirs et aux compétences numériques que nous mettons au cœur de nos travaux, avec des cycles d'auditions qui commenceront dans les jours qui viennent.

M. Jean-Claude Laroche, vice-président du Club informatique des grandes entreprises (Cigref). La souveraineté numérique est, depuis plusieurs années, un sujet

d'intérêt pour le Cigref. C'est une question qui fait débat au sein même du Cigref, entre ses différents membres, puisque les grandes entreprises adhérentes ont souvent une activité à l'échelle de la planète, partout dans le monde. La question de la souveraineté ne se pose donc pas de la même manière selon que nous regardons uniquement le périmètre du territoire national ou plus largement l'ensemble de la planète où nous pouvons exercer nos activités.

Pour les entreprises, être souverain signifie réussir à maîtriser ses choix et son avenir dans le domaine numérique. Cela suppose de disposer de composants numériques qui soient auditables et maîtrisés :

– auditables. Cela signifie, lorsque nous avons une relation contractuelle avec des fournisseurs de solutions, de services ou de systèmes numériques, que nous avons besoin de savoir si ces produits ou systèmes répondent à un certain niveau de sécurisation, ce qu'ils font, mais aussi parfois comment ils sont fabriqués par nos fournisseurs ou prestataires.

– maîtrisés. Cela signifie, lorsque nous faisons appel à une solution, que nous sommes très attentifs à ce que celle-ci fasse ce que nous souhaitons et ne fasse pas ce que nous ne souhaitons pas qu'elle fasse, et ce dans la durée.

Voilà comment nous définissons notre capacité à maîtriser les solutions numériques que nous utilisons.

Du point de vue des grandes entreprises et des administrations adhérentes du Cigref, la situation est aujourd'hui une situation d'extraordinaire dépendance. Nous sommes dépendants de toutes sortes d'acteurs et de solutions qui, très souvent, ne sont pas européennes. C'est vrai dans le domaine des logiciels. Typiquement, nous utilisons des systèmes d'exploitation tels que Windows, de Microsoft, et des suites bureautiques de Google ou de Microsoft comme Microsoft Office, Word, Excel, etc. Ces solutions sont américaines. Le moteur de recherche très souvent utilisé est Google. Il en va de même pour les outils de communication, comme vous le voyez bien vous-même, puisque vous utilisez pour la mission sur la souveraineté le produit Zoom. Nous disposons aussi de solutions comme Teams, BlueJeans, Verizon ou Skype, qui sont américaines. Notre dépendance est presque totale.

En ce qui concerne les matériels, la situation n'est guère plus brillante dans la mesure où, par exemple, nos *data centers* sont très souvent constitués de composants américains. Les routeurs dont sont munis les *data centers* de nombre de nos adhérents sont souvent de marque Cisco. C'est également vrai pour le matériel qui équipe les bureaux. Les ordinateurs personnels sont souvent fabriqués en Chine, avec des composants américains conçus et parfois développés en Israël.

Est-ce un problème pour notre capacité à maîtriser nos systèmes numériques ? Oui, c'est un problème notamment sur deux volets.

Le premier volet est une certaine fragilité dans la protection de nos informations. Plus nous faisons appel à des solutions tierces, notamment à des solutions développées dans des pays extra-européens et qui sont soumis à des juridictions extra-européennes, plus la protection des informations qui circulent dans ces composants techniques ou dans ces solutions représente un problème pour nous.

Le second volet concerne la *supply chain*. Au moment de la pandémie, par exemple, un certain nombre de nos adhérents se sont demandé s'ils réussiraient à s'approvisionner en

masse en ordinateurs portables pour assurer le passage en télétravail massif des salariés de leurs organisations.

La fragilité de la *supply chain* et celle de la protection de l'information constituent donc deux questions majeures pour les adhérents du Cigref.

Vous pouvez me dire que ces questions concernent les entreprises, mais qu'elles ne sont pas vraiment des questions de souveraineté. Comment abordons-nous, au Cigref, la question de la souveraineté ? Pour nous, la souveraineté est avant tout un attribut des États, plus que des entreprises. La souveraineté est *a priori* la capacité des États à exercer leur pouvoir sur une zone géographique donnée et une population donnée mais, évidemment, l'espace numérique est un espace particulier. En effet, la notion de territorialité dans l'espace numérique est différente de celle de l'espace physique. Les notions de frontière n'existent pas, ou pas de la même manière, et je ne parle même pas des questions d'identité. La question de l'identité numérique est une question en tant que telle.

Nous nous sommes donc interrogés pour savoir ce que nous pouvions entendre par souveraineté numérique. Pour nous, la base de l'exercice de la souveraineté dans l'espace numérique est la capacité à assurer la sécurité des biens et des personnes qui fréquentent l'espace numérique, la capacité à assurer la sécurité des activités légales des entreprises et des administrations publiques. Nos adhérents, clairement, ont besoin d'être en sécurité lorsqu'ils utilisent le cyberespace. Ils ont besoin que les autorités nous assurent que nous exerçons nos activités en sécurité, c'est-à-dire que les autorités garantissent l'ordre public dans cet espace. Au fond, les grandes entreprises et les administrations adhérentes du Cigref ont besoin que le cyberespace soit un espace de droit, dans lequel on fasse respecter le droit.

De notre point de vue, il existe un déficit dans la capacité des États – de l'État en France, mais pas seulement – à assurer cette sécurité dans le cyberespace. La capacité des États à assurer une forme de souveraineté sur l'espace de leurs propres ressortissants utilisant le cyberespace est clairement en retard par rapport à la rapidité du développement des usages du numérique et l'augmentation du niveau de dépendance de nos entreprises et de nos économies à l'égard du numérique. Nous avons besoin que les pouvoirs publics développent les outils de la puissance publique pour garantir cette base qu'est la sécurité de l'exercice de nos activités dans l'espace numérique. Cela suppose évidemment une volonté politique.

Dans quelle mesure la crise sanitaire a-t-elle modifié la perception que nous avons de la notion de souveraineté et de nos besoins dans ce domaine ? La crise sanitaire a un peu bouleversé la donne sur deux sujets et d'abord celui des usages. Elle a provoqué une explosion des usages du numérique dans tous les domaines. Cette tendance concerne aussi bien les étudiants qui suivent leurs cours au moyen des outils numériques que les personnes qui ont besoin d'un ordinateur pour accéder aux services de l'administration et parfois même tout simplement pour faire des courses et se faire livrer. Nous avons aussi constaté une explosion du télétravail et il faut des outils numériques pour télétravailler. Nous avons donc besoin de faire transiter de l'information, parfois sensible, à travers des réseaux et des systèmes qui nous permettent de travailler à distance.

Sur le plan des technologies, cette évolution a mis en évidence la centralité du *cloud*, de l'informatique en nuage, pour pouvoir exercer son activité depuis n'importe quel terminal, depuis n'importe quel lieu, à n'importe quel moment. C'est le *cloud* qui le permet en termes d'infrastructures. Il s'ensuit le besoin urgent d'un *cloud* de confiance pour les grandes

entreprises et les administrations françaises, de sorte que nous puissions travailler à distance, sur la base d'infrastructures partagées dans le *cloud* et en toute sécurité.

Que signifie un *cloud* de confiance ? Volontairement, nous ne parlons pas de *cloud* souverain, puisque toutes sortes de technologies peuvent se trouver dans un *cloud*, y compris des technologies américaines, israéliennes… Nous avons essayé de définir un *cloud* de confiance, d'abord comme un *cloud* immune au droit extra-européen. Typiquement, il ne faut pas qu'un juge d'un pays extra-européen puisse s'appuyer sur la législation de son État pour aller regarder les données hébergées dans le *cloud* d'une entreprise qui serait considérée comme extra-européenne et appartenant à cet État.

Deuxièmement, un tel *cloud* doit être sécurisé avec tout ce que cela suppose en matière de cybersécurisation.

Troisièmement, un tel *cloud* doit permettre d'entretenir une relation de confiance avec le prestataire du *cloud*, c'est-à-dire répondre à des besoins de réversibilité – la capacité à récupérer ses données et à les porter ailleurs, dans un autre *cloud*, pour faire jouer la concurrence – ainsi qu'offrir une véritable portabilité des données et une auditabilité de la solution.

Un tel *cloud* de confiance permettrait d'héberger également des solutions collaboratives de grands hyperscaleurs américains. Pour nous, le fait que le *cloud* ait ces caractéristiques ne signifie pas qu'il n'héberge pas de solution extra-européenne ; il pourrait héberger n'importe quel type de solution, mais en les protégeant suffisamment pour que nous soyons assurés, en utilisant ce *cloud*, de la relative immunité des données qui s'y trouvent.

Nous exprimons également des besoins dans d'autres domaines pour accroître une certaine forme de souveraineté, c'est-à-dire de maîtrise de l'espace numérique. L'État en France pourrait être beaucoup plus volontariste dans la promotion de l'*open source*. Il offre des solutions parfois tout à fait compétitives comparées aux solutions des grands éditeurs de logiciels, y compris dans le domaine des suites bureautiques. Ces solutions sont utilisées par l'administration, mais il faut en faire une véritable promotion pour que les acteurs autres que les acteurs publics s'en emparent, les utilisent, les apprécient, aident à les améliorer, y compris dans les communautés de développeurs. La promotion de l'*open source* constitue une des voies qui nous permettrait de limiter notre dépendance à l'égard des grands acteurs extra-européens en matière de solutions logicielles.

Je prends un exemple : nous sommes sur Zoom aujourd'hui. Comment imaginer que, avec de très grandes entreprises de services numériques comme nous en avons sur le territoire national, nous ne soyons pas capables, au niveau national ou européen, de développer une grande solution de visioconférence qui soit largement partagée et utilisée ? Cela nous interroge.

Pour les grands acteurs, la visioconférence est un outil de pénétration auprès de l'ensemble de la population. Tout le monde a besoin d'une visioconférence aujourd'hui. Pour un acteur tel que Microsoft ou Verizon, s'imposer comme ayant la solution la plus facile à utiliser, la meilleure est un vecteur de pénétration extraordinaire et, pour nous, c'est un vecteur de dépendance extraordinaire. Au même titre que l'État a fait un gros effort pour TousAntiCovid, pourquoi ne pas avoir fait l'équivalent pour la visioconférence ?

D'autres aspects nous permettraient d'améliorer notre souveraineté, comme la protection de nos pépites. Nous avons quelques entreprises qui sont de véritables pépites et qui, malheureusement, se vendent au plus offrant pour se développer. Elles se vendent souvent à des acteurs extra-européens.

Je prends deux exemples récents. J'ai été personnellement frappé de voir le rachat de l'entreprise Sentryo par Cisco. Sentryo était spécialisée dans la cybersécurisation des systèmes d'information industriels. Cisco a proposé à Sentryo en la rachetant un financement lui permettant de développer ses activités, mais celles-ci ne sont plus françaises ou européennes. Plus récemment, Alsid qui est également une vraie pépite spécialisée dans la sécurisation des annuaires, des composants sensibles de nos systèmes d'information, a été rachetée par Tenable, une société américaine. La question de la protection et du financement de nos *start-up* offrant des solutions innovantes touche donc pour nous à la souveraineté.

Enfin, pour reprendre un peu de maîtrise des questions matérielles dans le domaine du numérique, il faut pour nous repartir de la base : l'industrie du microprocesseur. Il faut savoir si, au niveau européen, il y a aujourd'hui matière à relancer une industrie du microprocesseur pour ne pas laisser l'exclusivité de ces domaines à Israël, aux États-Unis et à la Chine.

Si nous voulons partir à la reconquête d'une certaine forme de souveraineté dans le domaine du numérique, nous pensons qu'il nous faut un véhicule pour ce faire. Nous l'avons fait à la Libération dans le domaine du nucléaire avec le Commissariat à l'énergie atomique. Pourquoi ne pas créer un organisme porteur des enjeux de recherche et développement dans le domaine du numérique ? Il nous permettrait de déterminer dans quels domaines nous voulons investir fortement, de tirer l'ensemble de l'écosystème numérique français et européen autour d'un certain nombre de choix d'investissements lourds. Notamment, si nous voulons redevenir présents dans le domaine des microprocesseurs, cela nécessiterait un véhicule pour y réfléchir et agir.

En introduction, vous avez parlé de la cybersécurité. La sécurisation du cyberespace repose pour nous sur quatre piliers :

– la cybersécurité elle-même, pour laquelle le plan d'accélération cyber de l'État va dans la bonne direction ;

– des questions de police et de justice pour appréhender les cybercriminels, et il nous semble que les moyens de la police et de la justice dans ce domaine ne sont pas à la hauteur du niveau des attaques et des menaces ;

– la question de la lutte informatique offensive et de son articulation avec la cybersécurité, de façon à neutraliser les cybercriminels et avoir la capacité d'aller les chercher pour détruire leur activité. C'est pour nous une prérogative des États, donc un volet de la souveraineté ;

– la sécurité des produits et services commercialisés partout, alors qu'ils ne disposent parfois d'aucun label permettant de s'assurer que ces produits et systèmes ne sont pas vulnérables ou potentiellement utilisables dans le cas d'attaques cyber.

Des textes européens ont été publiés récemment, notamment le *Digital Markets Act (DMA)* et le *Digital Services Act (DSA)*. Le Cigref n'a pas vraiment étudié le *DSA*, qui n'est pas directement dans ses préoccupations. Nous avons davantage travaillé sur le *DMA*.

Enfin, les besoins de formation sont criants en nombre. Pour former beaucoup plus, il faut intéresser les jeunes gens et les jeunes filles au numérique, y compris très tôt dans les écoles. Les promotions actuellement formées dans ce domaine sont extraordinairement déséquilibrées, essentiellement masculines.

M. Philippe Latombe, rapporteur. Vous avez dit que la souveraineté est l'apanage des États et non des entreprises. En revanche, n'est-ce pas tout de même celui des entreprises, dès lors qu'elles doivent travailler avec des données à caractère personnel, notamment à la lecture des arrêts de la Cour de justice de l'Union et du Règlement généralsur la protection des données (RGPD) ? Cette souveraineté ne devient-elle pas une obligation pour les entreprises dès qu'il s'agit des données personnelles ?

M. Henri d'Agrain, délégué général du Cigref. Il ne s'agit pas de séparer les responsabilités des entreprises de la responsabilité des États en matière de souveraineté. Pour le Cigref, lorsqu'une entreprise se pose la question de sa propre souveraineté, le premier point concerne la maîtrise de ses dépendances et le deuxième l'utilisation de solutions maîtrisables et auditées. C'est le cœur de la souveraineté vue d'une entreprise.

En revanche, lorsque les entreprises disent que la souveraineté est d'abord un attribut des États, elles pensent à celui qui dispose de la compétence de régulateur et doit assumer ses responsabilités. Il s'ensuit, bien entendu, pour les entreprises, des obligations réglementaires, légales. Il ne s'agit pas de contester leur responsabilité pour traduire dans leur fonctionnement les obligations réglementaires qui s'imposent à elles, notamment dans le domaine des données personnelles.

M. Jean-Claude Laroche. S'agissant du RGPD, nous appliquons un texte qui s'impose à nous, mais dont nous ne sommes pas les initiateurs. Discuter, voter, promulguer et faire appliquer un texte de cette nature est de la responsabilité des États et du législateur, non des entreprises. En revanche, les entreprises ont la responsabilité de se mettre en conformité avec le texte, et c'est ce que nous essayons de faire.

M. Philippe Latombe, rapporteur. L'invalidation du *Privacy Shield* par la Cour de justice de l'Union nécessite-t-elle une clarification sur un certain nombre de sujets ?

M. Jean-Claude Laroche. Nous sommes dans une zone d'incertitude extrêmement préjudiciable à nos activités. Typiquement, un DSI comme moi devant héberger des données personnelles et voulant faire appel à une solution américaine aurait, depuis l'invalidation du *Privacy Shield*, de démontrer que la protection des données par l'entreprise extra-européenne choisie est au moins du même niveau que celle imposée sur le territoire européen par le RGPD. Toutefois, la relation contractuelle que peut avoir un adhérent du Cigref avec un hyperscaleur comme Amazon Web Services, Microsoft ou Google est une relation du faible au fort. Il est évident que, même avec le maximum de « blindage juridique », il est extrêmement difficile de démontrer que Google exercera sa propre activité, dans ses propres *data centers*, sur un territoire extra-européen, dans des conditions me permettant, à moi DSI d'une entreprise française, de garantir que le niveau de protection des données est équivalent à celui du RGPD.

Cette invalidation transfère aux responsables des entreprises françaises une responsabilité qu'ils ne sont pas capables d'assumer et pour laquelle ils ne disposent pas des outils juridiques qui leur permettraient d'être sereins.

Les entreprises qui avaient déjà hébergé des données à caractère personnel dans des *clouds* américains se trouvent dans une espèce de vide juridique avec des risques pour elles. De notre point de vue, cette situation mérite une clarification et plonge dans l'insécurité les entreprises potentiellement utilisatrices de solutions dans des *clouds* extra-européens.

M. Henri d'Agrain. L'invalidation du *Privacy Shield* a plongé l'ensemble de nos adhérents, qu'il s'agisse des entreprises publiques ou privées, dans une situation de grave insécurité juridique. Nous avons posé plusieurs fois la question aux autorités publiques, tant françaises qu'européennes, pour demander une analyse de risque de la situation et l'élaboration de recommandations pour les entreprises. Les quelques recommandations que nous avons pu obtenir, notamment de la part de la Commission nationale informatique et libertés (CNIL), ne sont pas rassurantes sur la capacité des entreprises à les mettre en œuvre.

M. Philippe Latombe, rapporteur. Au niveau européen, des recommandations sur la protection des données ont été émises récemment. Ne vous suffisent-elles pas aujourd'hui ? Avez-vous besoin de clarifications supplémentaires ?

M. Henri d'Agrain. Absolument.

M. Jean-Claude Laroche. C'est l'une des raisons pour lesquelles le Cigref met autant d'énergie à animer les réflexions liées à GAIA-X, d'une part, et, d'autre part, à promouvoir l'idée qu'il faut aller rapidement vers un *cloud* de confiance. Nous ne pouvons pas rester durablement dans cette situation. Le *cloud* est l'instrument du numérique d'aujourd'hui et de demain. Il faut pouvoir l'utiliser de manière sereine, en se disant que les données mises dans le *cloud* sont suffisamment protégées. Nous avons besoin d'une offre industrielle qui permette d'assurer un niveau de confiance suffisant dans le *cloud*. Ce niveau de confiance n'existe pas aujourd'hui et le niveau d'insécurité a augmenté avec l'invalidation du *Privacy Shield.*

M. Philippe Latombe, rapporteur. Nous avons auditionné deux des trois plus grands *clouders* américains, Amazon Web Services (AWS) et Google. Les deux ont tenu des propos extraordinairement rassurants, expliquant à quel point ils étaient intégralement en conformité avec la réglementation et ne comprenant pas pourquoi nous nous posions encore des questions.

Nous avons même eu la semaine dernière une interprétation d'IBM nous disant : « Nous ne sommes pas américains, nous sommes français puisqu'IBM France est une société de droit français. »

AWS et Google nous ont confirmé que, pour eux, toute filiale européenne des groupes américains était soumise au *Cloud Act* comme tout le monde. Cette analyse générale, était la nôtre. En revanche, ils nous ont dit et redit ne pas comprendre pourquoi nous posions la question de zones d'incertitude.

M. Henri d'Agrain. Le 16 juillet dernier, la Cour de justice de l'Union européenne n'a pas invalidé le *Privacy Shield* au titre du *Cloud Act*, mais au titre de l'article 702 du *Foreign Intelligence Surveillance Act (FISA).*

Cela n'a rien à voir avec le *Cloud Act* Lorsque des entreprises comme IBM vous disent être immunes face au *Cloud Act*, ce n'est pas vraiment le problème, notamment pour des entreprises globales. Les entreprises globales qui ont des activités aux États-Unis sont de toute façon américaines aux États-Unis et donc soumises directement à la réglementation

américaine. Le principal problème pour les entreprises provient de réglementations très intrusives comme l'article 702 du *FISA*, ainsi que l'a très justement reconnu la Cour de justice de l'Union européenne.

M. Jean-Claude Laroche. D'autres législations américaines sont susceptibles de poser de graves problèmes à nos adhérents. Le *Foreign Corrupt Practices Act (FCPA)* permet à un juge américain de rechercher des échanges de mails entre personnes d'une même entreprise pour, par exemple, convaincre de corruption quelqu'un qui, arrivant sur le territoire américain, se ferait arrêter sans même comprendre pourquoi. Ce type de pratique plonge les dirigeants de nos entreprises dans une insécurité majeure.

M. Henri d'Agrain. C'est à ce titre que les adhérents du Cigref estiment qu'une partie significative de leurs données nécessitent des outils de confiance pour être hébergées et traitées dans le *cloud*. Ce ne sont pas uniquement des données personnelles, mais des données de toutes natures, stratégiques, financières, commerciales, contractuelles ou relevant de la propriété intellectuelle, de la recherche et développement.

Ces offres d'hébergement ne sont malheureusement aujourd'hui pas disponibles sur le marché. C'est pourquoi nous faisons la promotion du *cloud* de confiance auprès des pouvoirs publics, de nos partenaires européens et de l'Union européenne, dans le cadre de GAIA-X. Nous avons la conviction que le *cloud* ne constitue plus une technologie parmi d'autres, mais la technologie qui commande toutes les autres.

Les autres technologies, qu'il s'agisse du *edge computing* dont la Commission européenne parle beaucoup, de la 5G, de la 6G, de l'intelligence artificielle ou le *quantum computing*, se développeront de toute façon sur le *cloud* et ce dernier les commande.

Si la France et l'Europe veulent restaurer une forme de souveraineté, il faut commencer par se doter des fondements de ce qu'est le numérique : des processeurs souverains et un *cloud* souverain.

M. Philippe Latombe, rapporteur. Où en sommes-nous aujourd'hui de la numérisation des entreprises, en France et en Europe ? Sommes-nous au bon niveau d'offre ?

M. Jean-Claude Laroche. La numérisation des entreprises s'est considérablement accélérée ces dernières années. Il est difficile de dire, dans l'absolu, si nous sommes au même niveau que d'autres. Dans certains domaines, je pense que nous sommes plus avancés que d'autres et, dans d'autres domaines, cela dépend des entreprises. Certaines ont pris du retard mais, de façon générale, la numérisation des entreprises progresse. D'ailleurs, le Cigref accompagne ses adhérents, depuis plusieurs années, dans une numérisation rapide de leur activité.

La numérisation des activités tertiaires est très avancée chez les adhérents du Cigref. Nous nous situons maintenant dans une vague de rapprochement entre les technologies de l'information et l'informatique industrielle, qui était auparavant plutôt réservée à des systèmes propriétaires, à des systèmes dédiés. Nous assistons à une convergence et à une numérisation des activités industrielles sensibles.

Cette numérisation de tous les secteurs d'activité de nos entreprises et de nos administrations, y compris les activités sensibles, pose la question de la cybersécurisation de ces activités et de la résilience de nos économies.

Nous ne sommes pas en retard, loin s'en faut. Par exemple, en matière de déploiement des comptages communicants, nous sommes plutôt en avance.

M. Philippe Latombe, rapporteur. Quand une entreprise – petite et moyenne (PME), très petite (TPE) ou de taille intermédiaire (ETI) – veut se numériser, dispose-t-elle du bon niveau d'offres ? Trouve-t-elle des solutions qui lui permettent d'avoir une réflexion complète sur sa numérisation, en intégrant la question de la cyber ?

M. Henri d'Agrain. Le Cigref s'exprime pour ses 150 adhérents, qui sont essentiellement de grandes entreprises françaises du CAC 40 et du SBF 120, ainsi que de très grandes administrations publiques françaises. Il réserve ses activités à des acteurs qui ont des effets d'échelle et d'importance particulièrement élevés. Nous avons peu de visibilité sur les produits qui existent pour les PME, TPE et ETI.

M. Jean-Claude Laroche. La réponse que je vous ai donnée sur le niveau de numérisation des entreprises portait sur nos adhérents.

M. Philippe Latombe, rapporteur. Je vous pose la question, car un certain nombre de PME ou d'ETI sont des sous-traitants ou des fournisseurs importants de vos entreprises. Cette numérisation, qui peut leur être imposée, ou être rendue nécessaire par vos relations commerciales avec ces sous-traitants, n'ouvre-t-elle pas des brèches, en termes de sécurité, chez vos adhérents également ? Cette descente de la numérisation chez vos fournisseurs, qui n'est pas forcément accompagnée de la réflexion globale nécessaire, peut-elle créer des brèches dans la cybersécurité ?

M. Jean-Claude Laroche. Il est certain qu'un des éléments de fragilité de nos adhérents provient de leurs relations avec l'ensemble des acteurs qui les entourent, notamment leurs prestataires ou fournisseurs qui n'ont pas forcément le même niveau de sécurisation. C'est une évidence.

Au Cigref, nous considérons que nous avons une responsabilité, y compris dans les clauses contractuelles que nous mettons en place dans nos conditions générales d'achat, pour aider à hausser le niveau de sécurisation de l'ensemble du paysage autour de nous.

Les adhérents du Cigref commencent malgré tout par essayer de se soigner eux-mêmes : l'effort consenti ces dernières années, notamment en matière budgétaire, a été essentiellement concentré sur les systèmes d'information internes. Maintenant, petit à petit, nous étendons le champ des prérogatives, en particulier au travers de nos relations contractuelles.

Pour autant, vous avez raison. Le fait que la sécurisation de l'ensemble de l'écosystème soit liée à la sécurisation des maillons les plus faibles constitue l'un des facteurs de risques majeurs en matière de cybersécurité.

M. Philippe Latombe, rapporteur. Disposez-vous de suffisamment de personnes de talent pour répondre à l'ensemble de vos besoins ? Sinon, comment les trouvez-vous aujourd'hui ?

M. Jean-Claude Laroche. Avons-nous des personnes de talent ? La réponse est oui. En avons-nous assez ? La réponse est non. Le marché des personnes ayant un haut niveau de qualification dans le domaine de la cybersécurité est extrêmement tendu et, pour certains

types de compétences, les éléments de rémunération ont tendance à augmenter fortement, ce qui n'est qu'une traduction de la rareté de ces compétences.

Pour arriver à la hauteur de ce qui serait nécessaire, des efforts multiples s'imposent, depuis la création d'écoles cyber internes à nos adhérents jusqu'au travail effectué avec l'ensemble des acteurs de la formation pour qu'apparaissent les formations dont nous avons besoin et, surtout, qu'elles soient suivies par un nombre de personnes suffisant pour alimenter ensuite nos besoins.

Nos besoins sont déjà importants en situation courante mais, si une attaque systémique atteignait une vingtaine de grands acteurs français et qu'il fallait reconstruire des systèmes d'information, chez ces vingt acteurs majeurs, simultanément, la France serait en difficulté pour trouver les compétences nécessaires.

M. Henri d'Agrain. Les propos de M. Jean-Claude Laroche sur les compétences dans le domaine de la cybersécurité traduisent un déficit beaucoup plus large des compétences dans les métiers du numérique.

Nous sommes présents au niveau européen dans des groupes de travail sur les compétences digitales. Il ressort des différentes informations dont nous disposons que la Commission européenne estime qu'il manquera à l'horizon 2025 entre 500 000 et 700 000 praticiens du numérique à différents niveaux de formation.

Dans les métiers du numérique, nos adhérents constatent une difficulté croissante à accéder aux meilleurs talents sur un marché mondialisé où ces derniers peuvent arbitrer, et non nécessairement en faveur du pays qui les a formés. Nous constatons une fuite des talents de haut niveau hors de France et d'Europe.

Les entreprises sont par ailleurs assez attentives à la baisse progressive du niveau de formation, en tout cas des exigences académiques pour des ingénieurs à bac+5 en sciences dures – mathématiques, physique – et il faudrait que la France soit attentive à ne pas baisser le niveau d'exigence de la formation des ingénieurs, notamment ceux orientés vers les métiers du numérique. Cela concerne toute la chaîne et il faut également « embarquer » des enfants. Par exemple, le nombre d'élèves qui choisissent, en fin de seconde, la spécialité « Numérique et sciences informatiques (NSI) » est assez faible et très peu de filles figurent parmi eux. De plus, l'une des trois spécialités de première est abandonnée en terminale et, en fin de première, cette spécialité NSI ne se trouve pas en bonne position. Or ce sont ces étudiants qui, à travers Parcoursup, choisiront ensuite les voies de formation des métiers du numérique dans l'enseignement supérieur.

Toute la chaîne n'est pas suffisamment performante au profit de l'ensemble de ces métiers qui représentent les métiers de demain. Le nombre de filles est catastrophique et la tendance se dégrade même encore. Nous avons actuellement 15 % de femmes dans les métiers du numérique au sens large et, dans l'enseignement supérieur, elles sont à peine 10 ou 12 %. La mixité des métiers du numérique se dégradera donc mécaniquement. Il faut vraiment faire des efforts.

Soyons bien clairs : nous n'atteindrons pas la souveraineté numérique sans compétences pour porter tous ces enjeux. La formation est un enjeu majeur pour restaurer en France et en Europe une certaine souveraineté numérique.

M. Philippe Latombe, rapporteur. Nous sommes déjà en retard dans certains domaines du numérique. Pensez-vous que, pour certaines technologies d'avenir, dans lesquelles nous sommes peu ou pas présents, en termes de recherche ou de développement, nous devrions investir assez vite ? Les entreprises en auront besoin. Si nous prenons du retard, nous nous retrouverons demain dans la même situation que celle que nous connaissons aujourd'hui dans le *cloud*, avec des acteurs étrangers.

M. Henri d'Agrain. En matière de recherche, la France n'est en général pas en retard. En revanche, elle prend du retard, d'abord, dans sa capacité à peser sur les organismes de normalisation où la France et l'Europe sont trop peu présentes au regard de la présence de la Chine par exemple. L'entrisme dont Huawei a fait preuve au sein des organismes de normalisation de la 5G est absolument extraordinaire. La France n'est pas suffisamment présente dans ces organismes, par exemple pour l'intelligence artificielle.

Le second point concerne la capacité à développer les résultats de la recherche et développement en investissant, d'où cette idée d'un équivalent du commissariat à l'énergie atomique, capable d'articuler la recherche pour préparer l'avenir et les investissements pour mettre en œuvre ces technologies d'avenir, avec des pendants civils et un pendant sécuritaire autour de la cybersécurité. Ce serait un instrument pour renforcer la capacité de la France à être présente sur l'ensemble du spectre des technologies nécessaires pour assurer cette souveraineté.

M. Philippe Latombe, rapporteur. Vous avez évoqué les exemples de Sentryo et Alsid. Ce savoir-faire existait et, immédiatement, il est capté ou racheté par Cisco ou par un autre opérateur, plutôt américain. Cela signifie-t-il que, en France et en Europe, nous ne sommes pas capables d'empêcher ces pépites de partir et ces acquisitions au sein de la zone France ou Europe ?

M. Jean-Claude Laroche. Nous avons effectivement des personnes extrêmement créatives en France, capables d'apporter des activités nouvelles, de créer des pépites. C'est incontestable. Souvent, ces personnes arrivent à démarrer une activité, y compris à faire financer un premier stade de croissance de leur activité mais, dès qu'elles atteignent une certaine taille, elles n'arrivent plus à trouver matière à se développer suffisamment. Elles se heurtent à quantité d'obstacles.

Très franchement, le code des marchés publics ou la directive 2014-25 relative à la passation des marchés par des entités opérant dans les secteurs de l'eau, de l'énergie, des transports et services postaux induisent des manières d'acheter qui passent par des procédures longues, souvent pas très cohérentes avec la durée de vie de ces entreprises et la nécessité de trouver des marchés assez rapidement. Lorsqu'un marché est passé, ces entreprises deviennent extrêmement dépendantes d'un client, avec parfois des marchés trop gros pour elles. Cette mécanique est peu adaptée en matière d'achats, pour les aider à grandir à un rythme qui leur convienne, avec des niveaux de marché qui leur conviennent.

Elles ont donc du mal à placer leur offre et, de plus, lorsqu'elles veulent se développer et rechercher des marchés à l'international, elles ont beaucoup de mal, au-dessus d'une certaine taille, à lever ces capitaux à cet effet. C'est la raison pour laquelle elles recherchent des financeurs. Il existe dans le monde des entreprises qui « scannent » partout les personnes créant des activités innovantes et elles viennent les racheter ou leur proposer de les racheter.

C’est une difficulté pour nous, si nous nourrissons nos pépites pour qu’elles partent trop rapidement, sans que nous ayons le retour sur investissement pour la collectivité.

Certains pays ont une stratégie consistant à faire grossir les *start-up* pour qu’elles se revendent, y compris aux Américains ou autres. C’est le cas d’Israël. Toutefois, ils ne le font que lorsque les entreprises ont atteint une taille suffisante, sont au moins des licornes, de sorte que leur valorisation soit suffisante pour rapporter à l’économie du pays qui les a soutenues pendant la phase de croissance. Ils font en sorte que ces entreprises puissent grossir jusqu’au stade de la licorne. Nous avons visiblement un problème de ce côté.

Nous voyons des gens brillants, qui travaillent parfois à l’Agence nationale de sécurité des systèmes d’information (ANSSI) ou chez nous, dans nos propres entreprises, aller créer des *spin-off* de leur activité, créer une activité utile pour tout le monde. Ils arrivent à la faire grossir un peu et sont rachetés par d’autres. C’est un problème majeur si nous voulons donner à notre pays, et plus généralement à l’Europe, plus de force dans le monde du numérique.

C’est notre analyse en tant que clients. Ce n’est pas le résultat d’un rapport.

M. Philippe Latombe, rapporteur. Qu’attendez-vous aujourd’hui de l’État pour lever ces difficultés ? Quelles sont les mesures urgentes qu’il faudrait prendre ?

M. Jean-Claude Laroche. Nous avons besoin d’un dispositif permettant de mutualiser les besoins en *cloud* de confiance de la part des administrations et des grandes entreprises, de façon à ce qu’une offre industrielle puisse ensuite se construire. Cette offre industrielle exige, de la part de ceux qui l’apporteront, un engagement de capitaux donc une prise de risques qui n’est possible que s’ils ont un marché.

Nous avons donc besoin d’une mutualisation des besoins en *cloud* de confiance et d’une promotion de l’*open source*. Il faut aussi que les entreprises sur lesquelles nous nous appuyons, notamment pour les systèmes d’information essentiels ou les systèmes d’information d’importance vitale, qui sont des pépites nationales, disposent d’une relative protection juridique et ne puissent pas être préemptées trop rapidement par des acteurs américains par exemple. Nous aurions besoin que, dans le code des marchés publics, pour des besoins spécifiques, tels que ceux liés à la cybersécurité, quelques dispositions dérogatoires ou complémentaires au droit de la concurrence nous aident à flécher nos achats et nos investissements vers ces entreprises.

M. Henri d’Agrain. Je crois essentiel que l’État et l’Europe se mettent en mouvement pour réguler la sécurité dans l’espace numérique. Le premier pilier de la cybersécurité a fait l’objet d’un plan d’accélération qui est bienvenu. Il est particulièrement bien adapté me semble-t-il mais il reste trois autres piliers sur lesquels il faut également accroître la capacité de l’État et de l’Europe à réguler :

– la coopération policière et judiciaire pour appréhender, lorsque c’est possible, les cybercriminels ;

– la capacité de l’État à assurer la cyberdéfense en profondeur pour aller neutraliser les cyberattaquants là où ils sont lorsque nous ne pouvons pas les saisir. Si ce n’est pas l’État qui le fait, ce seront des milices privées avec le développement de stratégies de *hackback* qui ne correspondent pas à ce que les entreprises membres du Cigref peuvent attendre ;

– enfin, il faut développer la régulation de la sécurité des produits et services numériques. À cet égard, j'attire votre attention sur un rapport tout à fait intéressant de l'Organisation de la coopération et de développement économiques (OCDE) sur le renforcement de la sécurité des produits. Ce rapport contient une liste de recommandations pour les politiques publiques.

Assurer la sécurité dans l'espace numérique constitue la première responsabilité en matière de souveraineté des États, au même titre que dans l'espace physique. C'est en assurant ces quatre piliers que l'État en France, les États européens et l'Europe pourront garantir une certaine forme de souveraineté.

M. Jean-Claude Laroche. Nous aimerions que l'État rassemble les grandes entreprises de services numériques pour disposer d'une solution de visioconférence française ou européenne.

M. Philippe Latombe, rapporteur. L'État est parfaitement au courant. Nous avions des systèmes de discussion et d'échange en visioconférence qui n'étaient pas au niveau, mais nous ferons ce qu'il faut.

M. Henri d'Agrain. Vous aviez abordé la question du *DMA* sur lequel le Cigref est particulièrement engagé. Du point de vue de nos adhérents, c'est une opportunité absolument indispensable pour l'économie européenne. Nous ne travaillons pas seulement pour nos adhérents mais nous pensons que faire en sorte que le *DMA* permette de maîtriser la dépendance de l'économie européenne par rapport à des offres extra-européennes, aujourd'hui et encore plus demain, est vraiment d'une mission d'intérêt général. Il ne s'agit pas d'évincer les offres extra-européennes mais de maîtriser les taux de dépendance, la façon dont l'économie européenne sera complètement enfermée par ce type de solution. Si ces solutions ne sont pas européennes, je pense que nous aurons demain de grosses difficultés économiques.

Il faut se projeter à un horizon de dix ans, voir quelles sont les courbes de croissance du recours au *cloud* et à ces solutions pour soutenir l'ensemble des processus de l'économie, que ce soit pour les grandes, petites ou moyennes entreprises, pour les administrations publiques, locales ou pour l'ensemble de la vie de nos concitoyens sur le territoire de l'Union européenne.

Si nous ne parvenons pas à faire du *DMA* un instrument de régulation et de maîtrise de ces dépendances, nous serons passés à côté d'un enjeu majeur pour restaurer une forme de souveraineté numérique en Europe.

La séance est levée à 15 heures 30.

Membres présents ou excusés

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

Réunion du jeudi 18 mars 2021 à 14 heures 20

Présents. – M. Philippe Latombe.

Excusée. – Mme Frédérique Dumas.