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
8 octobre 2020
Séance de 11 heures

Compte rendu n° 4

SESSION ORDINAIRE DE **2020-2021**

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

ASSEMBLÉE NATIONALE

Audition, ouverte à la presse, de M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance, et de M. Mathieu Weill, chef du service de l'économie numérique

La séance est ouverte à 11 heures.

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

M. Philippe Latombe, rapporteur. Le président Jean-Luc Warsmann étant retenu, je me propose d'être à la fois président et rapporteur, jusqu'à son arrivée. Je me réjouis de votre présence, monsieur Thomas Courbe, directeur général des entreprises au ministère de l'économie. Votre réflexion viendra alimenter nos premiers travaux sur le thème de la souveraineté numérique. Vous êtes accompagné de monsieur Mathieu Weill, chef du service de l'économie numérique.

Plus que jamais, la souveraineté numérique est une affaire d'États mais surtout d'entreprises, comme nous le montrent le poids et l'influence des géants du numérique dans le monde. L'absence d'acteurs européens capables de rivaliser avec ces derniers et les difficultés de la puissance publique à réguler ces acteurs, particulièrement mobiles, en constituent deux illustrations. Je rappelle que les travaux de notre mission d'information porteront sur les thèmes des infrastructures numériques, de la fiscalité numérique, des technologies souveraines et de la cybersécurité, autant de sujets sur lesquels M. le directeur général, pourra utilement nous éclairer, sous un angle essentiellement économique et entrepreneurial.

Les entreprises sont en effet au cœur de notre réflexion sur la souveraineté numérique. Ce sont elles qui produisent les composants physiques du numérique et les solutions logicielles utilisées par des millions de personnes. Elles se transforment ou non grâce au numérique, ou doivent se prémunir contre le risque d'espionnage économique en protégeant leurs données. Elles sont aussi au cœur des attentes de nos concitoyens, qui manifestent une double exigence : plus de services numériques d'une part et plus de garanties pour la protection et l'usage de leurs données d'autre part, ce à quoi chaque régulateur national doit veiller.

Pour initier nos échanges, j'aimerais recueillir votre avis éclairé sur deux sujets qui nous occuperont ces prochains mois. Le premier est largement inspiré par notre actualité parlementaire et concerne le plan de relance et le programme d'investissements d'avenir (PIA). Nous nous trouvons en effet à un moment très particulier puisque nous essayons de tirer les enseignements de la crise sanitaire que nous avons traversée et qui reste d'actualité, notamment dans le domaine de la souveraineté numérique. La grande majorité de nos concitoyens et de nos institutions a souvent eu recours à des logiciels étrangers – américains dans leur majorité – pour poursuivre son activité pendant le confinement, avec les risques que nous connaissons tous, notamment en termes de cybersécurité. J'aimerais donc connaître le regard que porte la direction générale des entreprises (DGE) sur cette période. De quelles façons le plan de relance et le PIA intégreront-ils l'impératif de protéger ou de promouvoir notre souveraineté numérique ?

Le second sujet concerne l'Europe. De nombreux projets sont en effet en cours, aussi bien dans les domaines du *cloud* que de l'électronique, et plus globalement des technologies de pointe (technologie quantique, intelligence artificielle, *etc.*). Là aussi, je souhaiterais donc connaître la position et le regard de la DGE et disposer d'un état des lieux des forces et des

faiblesses de l'Union européenne face à ses concurrents directs, américains ou chinois notamment.

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Je vous remercie pour votre invitation sur ce sujet absolument essentiel. Je pense que votre introduction cerne parfaitement les enjeux de cette question de la souveraineté numérique, à la fois d'une manière structurelle mais aussi tels qu'ils ont été révélés par la crise.

À titre d'introduction, je vous propose de vous livrer la réflexion selon deux angles qui caractérisent, de notre point de vue, la souveraineté numérique. Il s'agit à la fois de la capacité à établir les règles qui permettront d'utiliser le numérique, de contrôler les impacts de ses usages et de disposer de l'autonomie sur les principales technologies qui vont conditionner ces usages du numérique. Vous avez à juste titre rappelé que ces usages étaient croissants et critiques dans certaines circonstances, comme celles connues au printemps.

Cette définition des règles me semble recouvrer trois enjeux, que vous avez d'ailleurs abordés dans cette introduction.

Le premier est la production de règles permettant d'assurer la sécurité. Nous avons récemment franchi une étape importante avec la loi sur la sécurité des réseaux 5G de télécommunication. Cette étape, d'ailleurs inspirante pour d'autres États membres, permet de garantir que le déploiement de la 5G et des réseaux correspondants s'effectue dans des bonnes conditions de sécurité. Le Gouvernement a donné un certain nombre d'autorisations, certaines avec des réserves matérialisant le fait qu'une analyse au cas par cas a permis de définir les cas où les réseaux 5G pouvaient être déployés sans restriction et d'autres avec certaines restrictions.

Le deuxième élément concerne la sécurité des données. Vous l'avez évoquée, il s'agit d'une préoccupation croissante des citoyens et des entreprises. Cette préoccupation est légitime dans la mesure où les entreprises, particulièrement, stockent une part croissante de leurs données dans le *cloud*. Cette préoccupation est également légitime car des législations étrangères, notamment américaines et chinoises, permettent de donner accès aux données hébergées dans des *clouds* à certaines autorités. Une réponse doit donc être apportée en termes de sécurisation des données. Suite au rapport de votre collègue Raphaël Gauvain sur la question, nous menons une réflexion sur la loi de blocage qui, rénovée ou appliquée de manière plus précise, pourrait constituer une réponse à cet enjeu de sécurité des données. Ces derniers mois, nous constatons d'ailleurs un recours croissant à la loi de blocage par les entreprises françaises. Nous avons observé une très forte augmentation des demandes de mobilisation de la loi de blocage. Je pense que cela témoigne, comme vous l'avez évoqué, de cette sensibilité croissante des entreprises à la nécessité de protéger leurs données, notamment dans le cadre d'instructions et de procédures à l'étranger.

Le troisième enjeu, sans doute le plus important dans cette définition de règles, est la régulation des grands acteurs structurants du numérique et des plateformes structurantes. Ces plateformes sont, aujourd'hui, pour un petit nombre d'entre elles, sont dans une position de *gatekeepers,* de contrôle très profond du marché sur lequel elles se trouvent. On constate que ce contrôle du marché emporte des externalités négatives extrêmement fortes, sur le plan économique, sur les questions de partage de la valeur et, plus globalement, sur le fonctionnement des sociétés. En effet, elles ont un impact sur les libertés individuelles, l'accès à l'information, la capacité des États à réguler la diffusion de certaines informations illicites

ou créant des difficultés. Sur ce sujet, qui n'est pas nouveau mais dont l'importance est croissante pour nos sociétés sur les plans économique et sociétal, il me semble que nous assistons à une prise de conscience forte de l'Union européenne. Une proposition est en cours d'élaboration par l'Union européenne dans le cadre du *Digital Services Act* (DSA), devant donner lieu à une proposition en fin d'année. Depuis plusieurs mois, nous travaillons très activement sur cette proposition afin de l'orienter pour qu'elle permette de disposer vraiment d'une régulation exemptée des grandes plateformes structurantes. De notre point de vue, cette régulation sera la seule véritablement efficace. Nous pensons que cette proposition permettra à la fois d'assurer un bon partage de la valeur sur tous les marchés où ces plateformes agissent ; de permettre à l'innovation de continuer de prospérer et d'éviter des effets de contrôle de marchés, inaccessibles aux acteurs innovants en raison de ce contrôle par les plateformes ; de traiter des questions spécifiques comme celles des places de marché, de leur responsabilité dans les produits qui sont vendus, leur qualité et parfois leur caractère licite ou non ; de traiter de la régulation des contenus, appelant des réponses au niveau européen – point qui dépasse le domaine de l'économie.

Le deuxième volet de la souveraineté numérique est finalement celui de la maîtrise des technologies. Nous constatons que tous les usages du numérique sont conditionnés par un certain nombre de technologies. Il nous semble que six d'entre elles sont critiques et constituent nos priorités pour assurer cette souveraineté numérique.

La première est celle des semi-conducteurs et de la microélectronique. Nous voyons bien, suite à des déclarations récentes du gouvernement américain, que ce sujet fait l'objet d'une mobilisation internationale. Il est devenu stratégique et a dépassé le seul champ de la technologie et de l'industrie pour devenir un vrai sujet de souveraineté au sens global. L'Europe n'a pas attendu pour avancer sur le sujet, avec les deux plans Nano successifs, qui doivent permettre de renforcer le tissu industriel européen sur la microélectronique. Suite à la crise, nous réfléchissons avec les Allemands et la Commission européenne à une accélération de ces soutiens à l'industrie de la microélectronique au niveau européen. Dans le cadre du plan de relance, nous avons déjà lancé des actions spécifiques sur certains aspects. Par exemple, dans le plan de relance automobile, nous avons un axe de soutien à l'innovation sur l'électronique de puissance, l'un des sujets particulièrement importants. Dans le cadre de nos efforts sur la résilience de l'économie, et en particulier sur des projets de relocalisation, nous avons lancé un appel à projets, fin août, qui doit viser particulièrement des projets de relocalisation de production de composants de microélectronique en France.

La deuxième technologie essentielle est le supercalcul. En France, nous avons Atos, qui est un champion européen et mondial du supercalcul, très impliqué dans les programmes européens. Nous allons prochainement présenter une stratégie sur le quantique et la manière dont on peut préparer le passage à l'accélération puis au calcul quantique, dans la continuité de tout ce qui est déjà fait sur le calcul haute performance. Ce calcul quantique constituera un élément de technologie essentiel pour la souveraineté numérique dans les prochaines années, pour des questions bien connues de performance mais aussi de sécurité. En effet, l'un des enjeux du calcul quantique sera la résilience des systèmes de cryptage et donc des systèmes de sécurité actuels.

La troisième priorité est, évidemment, l'intelligence artificielle. Nous avons déployé une première phase de notre stratégie d'intelligence artificielle depuis 2017. Nous avons engagé une deuxième phase sur un certain nombre de sujets qui nous semblent prioritaires et sur lesquels il est nécessaire d'accélérer. Parmi ces sujets se trouve, par exemple, l'intelligence artificielle embarquée, qui deviendra un élément essentiel dans les prochaines

années. En effet, l'intelligence artificielle sera de plus en plus embarquée dans les dispositifs mobiles, tels que nos téléphones ou l'internet des objets. Au lieu d'être concentrée dans des *clouds* comme aujourd'hui, l'intelligence artificielle sera intégrée directement dans les outils. En France, nous avons à la fois une recherche en intelligence artificielle très performante et des compétences en microélectronique qui permettent d'être performants en termes d'intelligence artificielle embarquée. Il s'agit donc un secteur où il est tout à fait crédible qu'avec les soutiens appropriés, nous puissions produire des acteurs de premier rang. Il s'agit d'une priorité sur ces sujets d'intelligence artificielle.

La deuxième orientation sur l'intelligence artificielle porte sur l'intelligence artificielle de confiance. Nous voyons bien que le numérique crée des sujets assez nouveaux dans la relation de confiance, à la fois pour les entreprises et pour les citoyens. Je crois qu'il s'agit de l'un des objets de votre mission. Nous avons engagé un grand défi d'innovation de rupture sur la manière dont on peut certifier les algorithmes d'intelligence artificielle. Le but de cette certification est d'apporter un modèle de confiance, à la fois pour les entreprises et pour les citoyens. Il s'agirait d'une manière de garantir le fonctionnement de ces algorithmes. De notre point de vue, cela constitue aussi un élément de différenciation pour la production d'intelligence artificielle en Europe, par rapport à d'autres acteurs moins sensibles à ces questions de priorités de confiance.

La quatrième priorité est le *cloud* et, plus généralement, la maîtrise de la donnée. Il s'agit d'une bataille difficile, face à des concurrents, notamment américains et chinois, très avancés. Il nous semble que des initiatives récentes permettront de consolider les acteurs européens et l'offre européenne de *cloud*. La première est l'initiative GAIA-X, menée avec les Allemands. Cette initiative permet notamment de répondre à un grand défaut des offres de *cloud* actuelles, en créant de l'interopérabilité et de la réversibilité. Aujourd'hui, dans la plupart des solutions de *cloud*, les clients – les entreprises notamment – sont en quelque sorte prisonniers de l'offre de *cloud* choisie. Les capacités à migrer d'une offre à une autre, donc à maintenir le pouvoir du client face aux autres offres de solutions sont assez réduites. L'un des enjeux de l'initiative GAIA-X est bien d'offrir un espace de marché, avec des solutions de *cloud* respectant un certain nombre de valeurs, en particulier ces valeurs d'interopérabilité et de réversibilité. Ces valeurs apporteront des garanties pour les clients de pouvoir faire évoluer leurs solutions au cours du temps. Nous pensons qu'il s'agira d'un élément assez différenciant. Il nous semble qu'il s'agit d'une place de marché sur laquelle des offres françaises et européennes de *cloud* pourront se développer et, peut-être, être mieux valorisées qu'aujourd'hui pour leurs clients.

Concernant le *cloud*, le deuxième enjeu est, là aussi, la confiance. La confiance est une ligne directrice de toute notre action sur le numérique. Vous l'évoquiez sur la sécurité des données face à un certain nombre de législations étrangères et face aux doutes généraux sur la manière dont les données sont utilisées. De notre point de vue, il est essentiel de développer des offres de *cloud* de confiance, apportant des garanties de ce point de vue.

Le troisième enjeu du *cloud* est le soutien du développement d'une offre la plus compétitive possible, pouvant rivaliser avec les autres offres, notamment américaines. Le Président de la République l'a abordé récemment dans une réunion avec les acteurs de la French Tech. Il peut s'agir d'offres collaboratives, sur lesquels nous avons déjà une belle offre française restant à fédérer, ou de services d'intelligence artificielle comme nous l'avons évoqué tout à l'heure.

La cinquième technologie critique, de notre point de vue, pour la souveraineté numérique est la cybersécurité. Vous l'avez abordée. Nous devrions prochainement présenter une stratégie d'accélération de l'offre française et européenne de cybersécurité.

La sixième priorité concerne les réseaux de télécom. La crise a particulièrement montré le rôle de ces réseaux de télécom, en particulier mobiles, dont nous pensons qu'il sera croissant dans l'économie et même dans la vie de nos sociétés. En Europe, nous avons la chance d'avoir deux acteurs, Nokia et Ericsson, parmi les leaders mondiaux. Il nous semble que le soutien de l'innovation dans ces domaines doit être une priorité, de même que l'anticipation des futures améliorations de ces réseaux. Au-delà des acteurs européens, il existe aussi un ensemble de start-up françaises très prometteuses dans le domaine des futurs réseaux télécom. Nous pensons qu'il est prioritaire d'assurer que des acteurs européens et français seront à même d'avoir des offres compétitives sur les réseaux de télécommunication.

Sur cette capacité à maîtriser la technologie comme un deuxième axe de la souveraineté numérique, toutes ces actions irriguent très fortement le plan de relance, et notamment son volet de soutien à l'innovation. Ce sera en particulier le cas pour tout ce qui sera financé dans le cadre du PIA, intégré dans ce plan de relance. Un certain nombre des stratégies que j'ai évoquées sur certaines de ces technologies seront soutenues par le plan de relance, y compris dans un cadre européen pour la plupart d'entre elles. Nous souhaitons, dans le cadre européen, promouvoir des *Important Projects of Common European Interest* (IPCEI). Les IPCEI sont ces nouveaux cadres d'action européens dérogatoires des régimes habituels d'aide d'État, expérimentés sur les batteries par exemple. Dans le domaine des batteries, ils ont finalement montré que l'on pouvait réintroduire une industrie nouvelle pour l'Europe. Nous voulons appliquer ces régimes sur le *cloud* et sur la microélectronique dans les prochains mois avec la Commission européenne, notamment dans le cadre d'un dialogue approfondi avec l'Allemagne.

Pendant de tout cet investissement dans le substrat des entreprises technologiques apportant l'offre pour le numérique, un volet défensif, de notre point de vue, le complète. Ce volet défensif nous a conduits à renforcer notre politique de sécurité économique ces dernières années. Cela nous a également conduits à mieux identifier notre patrimoine économique des entreprises les plus stratégiques, dont beaucoup se trouvent dans les différents domaines que j'ai cités. Nous avons renforcé notre capacité à identifier les menaces sur ces entreprises, notamment les risques de captation de technologies et de rachat par des entreprises étrangères susceptibles d'entraîner une perte de la maîtrise de ces technologies. Nous avons également renforcé les dispositifs de réponses à ces menaces pour nous assurer que, de manière pérenne, tout l'investissement que nous consacrons au soutien à l'innovation et au développement de l'offre de ces entreprises leur permette de rester souveraines et à la disposition des acteurs français et européens.

Je pense que les enseignements précis de la crise sont de trois ordres, que j'ai déjà quelque peu abordés dans cette stratégie de réponse sur la souveraineté économique.

Le premier est, évidemment, le besoin de renforcer les infrastructures numériques sur le territoire. Pendant la crise, nous avons constaté que ces infrastructures avaient tenu mais qu'elles étaient essentielles dans des situations de ce type. Dans une perspective où un certain nombre de comportements pourraient changer en matière de déplacements et de communication, nous identifions que le renforcement des infrastructures numériques sera absolument essentiel. Le financement de la généralisation de la fibre optique à 2025 est d'ailleurs un axe du plan de relance.

Le deuxième enseignement est le besoin que toutes nos entreprises adoptent les solutions numériques comme un élément essentiel de leur compétitivité. Dans les classements, la France est en général onzième en termes d'usage du numérique par les entreprises. Ce classement laisse donc des marges de progrès. Dans le cadre du plan de relance, nous voulons accélérer l'adoption des technologies numériques à la fois par les entreprises industrielles et par les plus petites entreprises. Le ministre chargé des petites et moyennes entreprises (PME) devrait lancer prochainement un plan de numérisation des plus petites entreprises, à la fois PME et très petites entreprises (TPE), pour assurer cette diffusion du numérique.

Le troisième axe est le besoin d'outils de confiance (*cloud* de confiance, outils collaboratifs de confiance) pour les acteurs, les citoyens et les entreprises. Vous l'avez évoqué et j'ai essayé d'y répondre sur l'offre technologique. J'ai essayé de tracer les perspectives de développement de cette offre, à la fois pour créer des offres de *cloud* apportant cette confiance et des outils, tels que la visioconférence, sur lesquels des garanties de confiance doivent être apportées. Ces outils doivent être ainsi plus largement sélectionnés qu'aujourd'hui par les entreprises pour leurs usages, qui seront croissants dans ce domaine.

M. le président Jean-Luc Warsmann. Merci. J'ai deux questions, l'une ponctuelle et l'autre beaucoup plus générale.

La question ponctuelle porte sur la fibre optique. On m'a cité le cas d'un cadre français, résidant en France et travaillant dans le secteur bancaire en Suisse, à qui du télétravail a été refusé, contrairement à ses collègues suisses. Son employeur lui a expliqué que le réseau français de fibre était beaucoup moins sécurisé que le réseau suisse. Par conséquent, il ne l'a pas autorisé à travailler depuis le réseau de fibre français. Avez-vous identifié le sujet ? Est-ce factuellement exact ? Cela m'a beaucoup étonné. Je me permets de vous poser cette question car vous parliez de réseaux de fibre.

Par ailleurs, si vous voulez voir un dossier exemplaire de mise en place de la fibre, la région Grand Est a organisé une concession avec très peu d'argent public. En ex-Alsace, il me semble qu'il y a 40 % d'argent public. Sur les sept autres départements et nouvelles régions, je crois que le chiffre s'élève à 15 ou 18 % d'argent public. Nous nous contentons donc de cette mise et le reste est aux risques et périls de l'exploitant pendant trente-cinq ans. Nous ouvrons le réseau dans des communes de trente habitants où les gens sont hébétés de voir la fibre qui arrive. Il est ainsi possible de conduire ces projets en respectant les délais et l'argent public.

Ma deuxième question porte sur un sujet beaucoup plus important. Vous avez abordé le sujet du capital des sociétés sensibles. Considérez-vous que les textes européens et français sont suffisants pour que l'on puisse protéger des ventes de sociétés sensibles aujourd'hui ? Ou existe-il encore des « trous dans la raquette » ?

Quant à mon deuxième point, l'existence massive des acteurs privés ne me pose aucune difficulté. Néanmoins, l'absence d'un acteur semi-public ayant une part d'actions me semble quelque peu problématique. En effet, lorsque vous injectez beaucoup d'argent dans une société, elle vaut évidemment beaucoup plus cher. Je souhaite le bonheur des dirigeants de la société et de ses actionnaires mais je ne serais pas contre l'idée que l'État en détienne une petite partie. Cela peut aussi se faire par la Caisse des dépôts. Cela pourrait être une réponse à la première question. Si la Caisse des dépôts a 25 % d'entreprises sensibles, en cas de changement de capital, elle y sera aussi. Ma deuxième question est à la fois sous l'angle de la protection et de l'enrichissement. En travaillant sur un autre dossier portant sur le plan

Juncker, j'ai constaté que des financements colossaux étaient apportés à certaines entreprises, provoquant un enrichissement de l'actionnaire. Il me semble que la puissance publique ne s'y retrouve pas tout à fait assez.

M. Philippe Latombe, rapporteur. Permettez-moi de compléter les questions du président. Nous avons eu une audition il y a quelques instants avec les représentants des semi-conducteurs notamment. J'aimerais citer l'exemple d'ARM et de Nvidia et savoir si l'idée d'une sorte de banque publique d'investissement (BPI) européenne pourrait être une solution afin de permettre à des acteurs européens ou à des sociétés européennes travaillant dans le même domaine de faire des acquisitions de cet ordre. Concernant ARM, la valorisation de l'opération est colossale, autour de 40 milliards de dollars. Il s'agit effectivement d'une opération lourde à porter. Une BPI européenne pourrait-elle avoir du sens et comment pourrait-on la créer ?

J'aimerais vous poser une deuxième question concernant l'extraterritorialité américaine. Quel regard portez-vous sur ce mode de fonctionnement américain ? Je ne parle pas simplement de l'extraterritorialité du dollar mais surtout des normes, en l'occurrence des licences imposées depuis deux ans.

Ma dernière question relève peut-être d'un épiphénomène mais elle est d'actualité. La Cour de justice de l'Union européenne (CJUE) a invalidé le *Privacy Shield*. On parle beaucoup de *cloud* mais on voit aussi que les entreprises ont aujourd'hui besoin de stabilité juridique. Quel est le regard que vous portez sur cette question, alors que nous nous trouvons dans un entre-deux ? L'ancien *Privacy Shield* n'existe plus mais le nouveau n'existe pas encore. Comment cela va-t-il fonctionner ? Quelles sont les menaces qui peuvent planer sur nos données pendant cette période ?

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Monsieur le président, au sujet de la différence entre la fibre suisse et la fibre française, il me semble que l'affirmation sur la sécurité est très discutable. La sécurité des données sur les réseaux dépend d'un très grand nombre d'éléments, relevant à la fois de la fibre elle-même mais aussi des *clouds*, des opérateurs et des équipements d'opération des systèmes. Je ne pense pas qu'il soit possible d'affirmer l'existence d'un déficit en la matière. En tout cas, il me semble que si l'on juge la sécurité dans laquelle un salarié opère, notamment dans le cadre du télétravail, le sujet ne se limite pas à la fibre et aux infrastructures. Il concerne également les outils utilisés et l'ensemble des solutions par lesquelles les données vont transiter. Tout ce que nous essayons de faire – que j'ai essayé de décrire en introduction – répond justement à l'idée d'offrir aux entreprises françaises un environnement numérique beaucoup plus sécurisé pour leurs données, à la fois sur le plan du stockage des données, des réglementations sur ce stockage et des questions de cybersécurité. Sur la cybersécurité, nous voyons bien qu'il faut améliorer l'offre.

M. Mathieu Weill, chef du service de l'économie numérique au sein de la direction générale des entreprises. Je confirme que, du point de vue technique, je ne vois pas en quoi il y aurait une moindre sécurisation de la fibre française par rapport à la fibre suisse. L'exercice de la profession dans un secteur bancaire peut laisser penser qu'il s'agit plutôt du risque d'extraterritorialité par rapport à des informations qui seraient manipulées. Cela nous nous ramène à la question relative à l'extraterritorialité du droit américain et donc à la protection de certaines données sensibles dans un contexte où elles passeraient sur un autre territoire que celui de la Suisse. J'imagine qu'il s'agit du fond de cette question.

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Vous citiez le Grand Est et le déploiement de la fibre en général. Concernant le déploiement de la fibre, nous avons et essayons toujours de trouver le bon équilibre entre ce qui peut être financé par le privé et ce qui doit nécessairement intégrer des financements publics. Je ne vais pas juger les réalisations dans chaque région mais il est vrai que, de ce point de vue, les résultats diffèrent en fonction des régions. Notre objectif est justement de permettre, grâce aux crédits prévus dans le plan de relance, d'assurer la généralisation du réseau *Fiber To The Home* (FTTH) dans toutes les régions, notamment dans celles qui ne l'auraient pas fait dans le cadre du plan actuel. En tout cas, notre objectif est bien d'assurer cette égalité territoriale.

Sur les outils pour protéger les entreprises, un texte réglementaire existe sur l'investissement étranger en France et sur le contrôle des investissements. Ce règlement repose juridiquement sur une exception au traité sur la libre circulation des capitaux. Pour cela, il nécessite de se rattacher à des enjeux de sécurité d'ordre public. Ces dernières années, nous avons beaucoup renforcé ce dispositif, en considérant que la sécurité et l'ordre public devaient être entendus dans une mission assez large. La Commission européenne ne nous a pas contredits sur ce plan. Au-delà de ce qui relevait à l'origine du secteur de la défense et de la sécurité à proprement parler, nous avons introduit tout un ensemble d'autres dimensions. Nous avons introduit toutes les infrastructures de réseaux, de transports et d'énergies. Avant la crise de l'épidémie de covid-19, nous avons étendu le champ à tous les secteurs numériques critiques. Nous avons introduit des secteurs tels que le *cloud*, le calcul haute performance ou l'espace. Nous avons donc pu élargir ces secteurs. Pendant la crise, nous avons ajouté, pour des raisons évidentes, le secteur des biotechnologies, dans le but d'accroître encore la palette des secteurs protégés. Nous avons également baissé le seuil d'intervention à 10 %. Si un investisseur étranger dans l'un de ces secteurs veut racheter une entreprise française à partir de 10 % du capital, nous avons la capacité de mettre en œuvre ce décret et donc de contrôler l'investissement.

Pour essayer de répondre à votre question, je pense que nous avons fait tout ce qui était possible au niveau national. Il me semble que nous avons maintenant une couverture très large des secteurs sensibles, et donc une capacité à y intervenir.

Au niveau européen, cette démarche est beaucoup moins avancée. Un règlement est entré en vigueur très récemment sur le contrôle des investissements étrangers. Ce règlement est plutôt du ressort de l'échange d'informations que de celui d'un vrai contrôle de l'investissement lui-même. Il me semble que l'Europe doit encore progresser pour, idéalement, aboutir à un dispositif similaire au nôtre, permettant vraiment de contrôler l'investissement et éventuellement d'imposer des conditions à l'investisseur.

Néanmoins, le contrôle de l'investissement ne peut pas constituer la seule réponse. Vous l'avez abordé, nous devons formuler également une réponse en fonds propres. Dans certains cas, il s'agit moins d'exercer un contrôle sur l'investissement que d'être capable d'avoir une offre française de rachat d'une entreprise donnée ou d'une start-up. Nous avons progressé ces dernières années sur ce point, avec la création d'une dizaine de fonds privés, suite au rapport de Philippe Tibi sur le financement des entreprises technologiques françaises. Ces fonds privés sont destinés à investir, en particulier dans les start-up. L'objectif affiché est de stabiliser ces start-up en France, d'éviter qu'elles soient achetées par un acquéreur étranger et d'éviter, comme on le voit souvent, que cet achat s'accompagne finalement d'un transfert de tout ou partie de l'entreprise à l'étranger. Nous avons donc une réponse privée, structurée ces deux dernières années et maintenant significative. Nous avons aussi une réponse publique,

bien sûr historique avec BPI, mais complétée pendant la crise avec le fonds French Tech Souveraineté. Ce fonds répond exactement, je crois, à l'objectif de votre mission. Il permettra d'apporter, pour l'État, des solutions en fonds propres, notamment pour des start-up stratégiques selon nous et sur lesquelles nous voudrons pouvoir intervenir en fonds propres pour permettre leur développement ou, de manière défensive, pour éviter qu'elles soient rachetées par un acteur étranger.

La question du partage de la valeur est très large. Soit par l'intermédiaire de la BPI soit de fonds publics tels que French Tech Souveraineté, l'État intervient en capital et est donc finalement rémunéré pour la réussite de l'entreprise. Pour le reste de nos investissements, notamment pour tout ce qui soutient financièrement l'innovation – axe important que j'ai évoqué – dans les entreprises privées, il nous semble que le retour sur investissement est très fort pour l'économie. C'est le cas dans la mesure où, évidemment, on ne finance que des projets et des innovations se réalisant en France. Il nous semble que la valeur économique créée par ces acteurs, plus forts et plus compétitifs, sera très importante pour le tissu économique. De notre point de vue, c'est l'essentiel du retour sur investissements sur l'État. En tout cas, parmi nos préoccupations, nous devons nous assurer, pour chaque projet individuellement, que les financements apportés auront bien un effet concret sur l'économie.

Le rachat d'ARM est évidemment très préoccupant. Il s'agissait d'un acteur européen très important sur l'architecture de calcul. Nous avons engagé une discussion avec la Commission européenne pour évaluer la pertinence de stimuler l'émergence d'un nouvel acteur d'architecture européen. En effet, aujourd'hui, nous ne pouvons plus considérer qu'ARM répond à notre objectif de souveraineté numérique. Il s'agit d'une discussion très récente, en cours. Cette question se pose légitimement, de notre point de vue.

Nous n'avons, aujourd'hui, pas la taille critique pour envisager la création d'une BPI européenne et des investissements considérables de ce type. Je crois que nous avons finalement, au niveau national, des outils permettant de répondre à peu près aux enjeux. Néanmoins, nous n'avons pas ces outils au niveau européen. Il s'agit d'un sujet sur lequel il n'existe pas de consensus européen. Je pense qu'un certain nombre d'États membres ne partageront pas l'idée que des volumes très importants de financements publics doivent être mobilisés dans des cas de ce type. Un débat européen doit donc avoir lieu, avant de progresser véritablement sur ce sujet.

Concernant l'extraterritorialité, une augmentation très forte de lois extraterritoriales – promulguées à la fois par la Chine et par les États-Unis – a été constatée ces dernières années. S'agissant de la Chine, nous l'avons constaté à travers l'application d'un certain nombre de sanctions étrangères, y compris les sanctions dites « secondaires » permettant finalement d'interdire une activité économique avec un pays sanctionné, sans qu'il n'y ait aucun lien avec les États-Unis. Un acteur européen peut être interdit même s'il n'existe aucun lien avec les États-Unis. Ce dispositif, purement extraterritorial, a été utilisé ces dernières années. Nous avons observé d'autres développements avec le *Cloud Act*, que j'ai déjà mentionné. Plus récemment, nous avons vu des restrictions d'exportation des composants, notamment de microélectronique. Ces restrictions sont très préoccupantes pour nos acteurs. Il s'agit là aussi d'un cas d'extraterritorialité dans lequel un acteur européen peut se voir interdire de commercer avec un acteur chinois, par exemple, alors même que ce commerce est tout à fait licite au regard de la législation européenne.

Nous portons ce sujet à Bruxelles, avec les autres États membres, pour essayer de mobiliser l'ensemble de l'Union européenne sur une réponse à ce sujet. La réponse serait

d'abord diplomatique. Il s'agirait ensuite d'examiner quelles sont les possibilités en droit. Il n'existe pas de réponse facile sur ce sujet pour avoir une réponse juridique permettant d'assurer la continuité des opérations commerciales. Finalement, la réponse de long terme est la souveraineté et la capacité à avoir la dépendance la plus faible possible par rapport à des acteurs non européens, dans nos productions et notamment dans le domaine du numérique en Europe. Ces restrictions américaines à l'export doivent nous encourager à poursuivre nos efforts pour combler les segments des chaînes de valeur numériques sur lesquelles il n'existe pas d'offre européenne. C'est cela qui permettra d'éviter cette dépendance. On voit bien le lien entre ce sujet et la souveraineté numérique.

Concernant l'extraterritorialité sur le *cloud*, j'ai évoqué la réponse que nous essayons d'apporter, avec le *cloud* de confiance. Ces derniers mois, nous avons pu matérialiser des offres non soumises à la législation américaine sur le *Cloud Act.* Ces offres permettront d'assurer aux clients européens que leurs données, hébergées dans des solutions de *cloud*, ne seront pas accessibles pour les autorités américaines dans le cadre du *Cloud Act*. Cela nous semble être la réponse technologique à l'extraterritorialité de cette loi.

Il n'existe pas de réponse facile concernant le *Privacy Shield.* Nous voyons potentiellement les conséquences de cette décision de justice sur la sécurité juridique des données. Il s'agit en même temps d'un sujet assez systémique. Nous poursuivons les discussions, à la fois avec l'Union européenne et avec les autorités responsables de la sécurité et de la protection des données européennes, afin de définir une réponse adaptée. Il n'existe pas encore de solution évidente pour rétablir rapidement une sécurité juridique complète sur ces sujets. L'essentiel reste à faire pour déterminer en quoi consisterait une solution pérenne, d'une part, et une solution transitoire, d'autre part, pour assurer la transition vers un nouveau cadre juridique assurant le même niveau de protection que le *Privacy Shield.*

M. Philippe Latombe, rapporteur. Je vous disais que nous avions interrogé avant vous les représentants de l'industrie des semi-conducteurs. L'un des représentants est partie prenante du problème puisqu'il est dirigeant chez STMicroelectronics. Il nous expliquait que les licences mises en place depuis le 17 septembre sont problématiques. En effet, des clients chinois font partie de ces clients les plus importants. C'est notamment le cas du client chinois visé. On voit bien que la volonté américaine est d'éviter que les clients chinois puissent avoir accès à certaines technologies. Au-delà de l'éventuel impact sur des acteurs américains qui ne pourraient pas vendre à leurs clients chinois, la conséquence de ces licences est une fragilisation des acteurs européens et français, privés de débouchés. À la DGE, quel regard portez-vous sur cela ?

Le chiffre d'affaires ayant tendance à baisser pour les entreprises concernées depuis le 17 septembre, un accompagnement sera-t-il apporté ? Si c'est le cas, quelle en sera la forme ? Comment essayerons-nous d'aider ces entreprises à maintenir leur chiffre d'affaires et donc leurs capacités à investir, à rechercher, *etc.* ?

Une autre solution semble possible. Avec l'Union européenne, pensez-vous passer par un intermédiaire d'État ou un intermédiaire européen ? Cet intermédiaire pourrait acheter à ces entreprises dans le but de revendre, sans être soumis de la même façon à l'obligation de licence des américains.

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Nous examinons les différentes options. J'ai rencontré l'ambassade des États-Unis la semaine dernière à ce propos. Nous avons initié de nombreuses

démarches auprès des autorités américaines, d'abord pour essayer de les convaincre de faire évoluer cette réglementation ou d'accorder des dérogations. Lors de situations précédentes, nous avons connu des cas dans lesquels les autorités américaines émettaient des interdictions de ce type puis accordaient ensuite des dérogations au cas par cas pour des entreprises européennes. Nous explorons cette voie.

Comme je l'indiquais tout à l'heure, nous regardons les autres options. À ce stade, nous n'envisageons pas d'indemnisation des entreprises concernées. Cet évènement est survenu récemment. Nous n'avons pas encore beaucoup de recul sur l'impact commercial réel. En tout cas, ce n'est pas l'option que nous étudions en priorité.

Avant de mettre en œuvre d'autres options (notamment le développement d'un intermédiaire), il faut vérifier que cela répond bien à l'enjeu. Le fait d'avoir un intermédiaire européen n'est pas forcément une solution permettant d'échapper aux interdictions de ces licences export. Tout cela est donc en cours d'analyse. Cependant, comme je l'indiquais tout à l'heure, il n'existe pas de solution évidente pour contourner ce problème. Nous poursuivons nos efforts vis-à-vis des autorités américaines pour cette raison.

Dans de nombreux cas concernant les questions de souveraineté numérique, nous constatons une sensibilité beaucoup moins forte des autres États membres, et dans une certaine mesure de la Commission européenne, sur ces sujets. Nous avons aussi besoin de convaincre la Commission et nos grands partenaires européens que ces sujets doivent être traités avec le niveau de priorité adéquat. Typiquement sur ces questions de licences export, nous n'avons pas encore cette mobilisation européenne des autres États membres, qui permettrait vraiment de progresser significativement.

M. Philippe Latombe, rapporteur. Selon vous, pourquoi les autres États membres n'ont-ils pas cette sensibilité ?

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Deux raisons me semblent l'expliquer. La première est que pour un certain nombre de nos partenaires, le bras de fer avec nos grands partenaires commerciaux, les États-Unis et la Chine, est peut-être moins spontanément envisagé qu'en France. Nous l'avons vu dans quelques sujets un peu comparables. Un certain nombre d'États membres craignent que ces sujets contentieux avec les grands partenaires commerciaux entraînent des rétorsions commerciales ou menacent leur position commerciale dans ces pays. C'est, à mon avis, l'une des raisons. Leurs arbitrages sont différents des nôtres sur ces sujets, nous empêchant d'avoir des positions communes.

Une deuxième raison plus fondamentale, que l'on retrouve sur tous ces sujets de souveraineté numérique, est que les autres États membres et leurs entreprises sont moins sensibles aux questions de confiance dans le numérique et de protection des données. Ces sujets existent évidemment mais sont, me semble-t-il, perçus comme moins critiques qu'en France.

Il me semble que ces deux raisons, l'une tactique et l'autre plus fondamentale, expliquent que, malgré une progression, il reste un grand effort de conviction à produire au niveau européen pour rallier la Commission et les États membres à nos positions.

M. le président Jean-Luc Warsmann. La dissuasion peut parfois être un moyen de conserver la paix. Quels sont les outils d'extraterritorialité dont nous disposons dans nos

réglementations, aux niveaux français et européen ? Utilisons-nous ces outils ? Devrions-nous « muscler » ces outils afin d'avoir l'équivalent de ce que peuvent faire les États-Unis ou la Chine ?

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. C'est effectivement une bonne question. Nous avons aujourd'hui très peu de dispositifs européens de nature extraterritoriale. Nous avons un règlement de blocage européen, datant des sanctions américaines des années 1960 et 1970, mais qui n'est jamais utilisé. Ce règlement de blocage serait d'ailleurs probablement difficile à utiliser. Il devrait être revu, dans le but d'une utilisation au niveau européen. Nous pensons que cela mérite d'être fait pour, comme vous le dites, nous doter d'outils permettant d'être un peu plus « à jeu égal ». Là aussi, nous avons la combinaison d'un sujet juridique de mise en œuvre d'un outil – devant sans doute être rénové – et d'une volonté politique variable parmi nos partenaires au sujet de l'utilisation de cet outil pour les raisons que j'ai évoquées – quand bien même serait-il disponible et complètement efficace. Il est vrai que l'Europe dispose de beaucoup moins de dispositifs. Il s'agit de l'un des seuls en Europe ayant cette dimension extraterritoriale.

M. le président Jean-Luc Warsmann. Dans le malheur du Brexit, nous perdons peut-être un pays ne nous aidant pas beaucoup à avancer dans ce domaine. Il sera peut-être plus facile d'avancer, même si nous regrettons évidemment la survenue du Brexit.

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Sans doute.

M. Philippe Latombe, rapporteur. J'aimerais vous poser une question de timing. Dans les différentes séquences qui arriveront les prochains mois, quelles sont les principales échéances que vous notez ? Le *Digital Services Act*, sur lequel vous travaillez, arrivera en fin d'année. Existe-t-il d'autres échéances aussi marquantes que celle-ci, sur lesquelles nous pourrions nous appuyer dans les prochains mois ? Qu'avez-vous dans votre « *scope* » et dans votre feuille de route ?

M. Thomas Courbe, directeur général des entreprises au ministère de l'économie, des finances et de la relance. Parmi les grandes échéances au niveau européen, le *Digital Services Act* est essentiel. Les mois à venir seront déterminants pour nous assurer que les propositions puis la négociation européenne conduisent bien à disposer d'une vraie régulation exemptée des plateformes structurantes. Un vrai travail, à la fois technique et de conviction, est nécessaire pour arriver à ce résultat. De notre point de vue, il s'agit d'un chantier essentiel pour l'Union européenne. Au-delà de l'échéance de cette fin d'année, la présentation du texte par la Commission, nous voudrions avancer assez rapidement dans la négociation pour nous doter du *Digital Services Act* le plus rapidement possible. Nous voyons bien que le pouvoir de marché des plateformes a des conséquences tous les jours sur les acteurs.

Les deuxièmes échéances concernent la construction de ces grands projets européens industriels sur l'offre numérique, le *cloud* et l'électronique. Ce sont, là aussi, des étapes importantes pour lancer une vraie mobilisation d'un grand nombre d'États membres et d'entreprises européennes, dans le but de créer des vraies chaînes de valeur comme ce qui a été fait pour les batteries, non seulement au niveau national mais aussi au niveau européen. Ces deux étapes, sur le *cloud* et sur la microélectronique, sont vraiment importantes. Nous espérons que nous pourrons avoir une vision claire et partagée avec nos partenaires et la Commission dans les prochains mois.

Au niveau national, la présentation de certaines de stratégies que j'ai évoquées aura lieu, notamment concernant la cybersécurité, le quantique et la santé digitale. La présentation sur la stratégie quantique sera bien sûr liée au niveau européen. La manière d'utiliser les outils numériques dans les systèmes de santé représente l'un des secteurs d'application particulièrement fort de la souveraineté numérique. Nous présenterons une stratégie sur ce dernier point afin d'initier une dynamique importante dans le domaine.

Plus tard, nous présenterons éventuellement une stratégie sur l'EdTech, soit les outils numériques dédiés à l'enseignement. Évidemment, la période du confinement nous a montré combien la capacité de formation par le biais des outils numériques était essentielle. Cela dépasse cette seule question pour embrasser, d'une manière plus générale, toute la question de la meilleure utilisation possible des outils numériques dans l'enseignement, depuis la maternelle jusqu'à l'enseignement supérieur. Sur ce sujet, l'offre française et européenne doit être structurée et soutenue dans son développement.

Ces étapes seront importantes dans notre stratégie de renforcement de l'offre française et européenne sur toutes ces technologies numériques. Il s'agit des principales étapes à court terme sur ces questions.

Autour de DSA, au niveau européen, il existe deux sujets concernant la régulation des plateformes. Le premier sujet est relatif aux places de marché. Nous souhaitons avancer dans la régulation des places de marchés, en particulier de certaines places non européennes servant d'intermédiaires à la vente de produits illicites. Le second sujet porte sur la régulation de contenu, sujet européen majeur sur lequel nous voulons apporter des solutions à relativement court terme.

La séance est levée à 11 heures 55.

Membres présents ou excusés

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

Excusés. - Mme Marietta Karamanli, Mme Laure de La Raudière, Mme Marion Lenne, Mme Nathalie Serre