N° 4299

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 29 juin 2021.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION (1)

sur le thème **« Bâtir et promouvoir une souveraineté numérique nationale et européenne ».**

ET PRÉSENTÉ PAR

M. JEAN-LUC WARSMANN, Président,

ET

M. PHILIPPE LATOMBE, Rapporteur,

Députés.

TOME II

CONTRIBUTIONS ÉCRITES ET DOCUMENTS COMPLÉMENTAIRES

COMPTES RENDUS DES AUDITIONS
(du 1er octobre 2020 au 9 mars 2021)

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » est composée de : M. Jean-Luc Warsmann, *président ;* Mmes Virginie Duby-Muller, Danièle Hérin, MM. Denis Masséglia, Jean-Michel Mis, *vice-présidents* ; M. Philippe Latombe, *rapporteur*, Mme Valéria Faure-Muntian, M. Philippe Gosselin, Mmes Marietta Karamanli, Amélia Lakrafi, *secrétaires* ; Mme Laetitia Avia, MM. Xavier Batut, Éric Bothorel, Moetai Brotherson, Mmes Frédérique Dumas, Paula Forteza, MM. Thomas Gassilloud Bastien Lachaud, Christophe Lejeune, Mme Marion Lenne, MM. Philippe Michel-Kleisbauer, Jérôme Nury, Pierre Person, Pierre-Alain Raphan, Mme Nathalie Serre, *membres*.

SOMMAIRE

—

Pages

CONTRIBUTIONS

Contribution de Mme Marietta Karamanli, députée et membre de la mission d'information

Contribution de Marietta KARAMANLI

Mission « Souveraineté numérique »

Un enjeu nouveau

Il y a, que l'on veuille ou non, une révolution des datas ; l'utilisation du numérique présent dans toutes les activités humaines conduit d'une part à rendre accessibles et capitalisables les données relatives aux activités mais aussi à modifier les activités par l'utilisation de données. Le secteur des soins ou l'éducation (le « care » aux personnes) en sont de bons exemples. Il existe des activités comme les activités de recherche clinique en santé (et sur les personnes) qui utilisent les données produites par l'essai pour adapter la dose ou la régularité du traitement.

Dans une économie globalisée les données intéressent tous les États et toutes les entreprises qui peuvent en faire leur matière première.

Il s'agit d'un élément essentiel même s'il ne faut pas se focaliser sur le seul risque qu'il emporte.

Clairement les données sont au cœur de la cyber défense et de la cyber sécurité. De plus en plus le mot et l'idée deviennent communs ; la surveillance, la défense et la sécurité existent dans l'espace numérique ; le cyber terrorisme et l'ensemble des menaces visant les systèmes stratégiques sont à l'œuvre depuis maintenant de nombreuses années.

Les États sont désormais confrontés au phénomène de « guerre hybride », une menace fondée sur la combinaison de moyens militaires et non militaires, notamment des

cyberattaques. Ce phénomène se développe autour d'une frontière perméable entre l'ingérence civile et l'attaque militaire.

Construire une souveraineté en soutenant fortement l'industrie du numérique

Pour des raisons multiples, les pays / États ont progressivement renoncé à leur industrie en évoquant une sorte de spécialisation dans la chaîne de valeur. Ici la matière grise et ailleurs la production (l'Asie étant en quelque sorte la « grande usine du Monde »).

Mais on l'a constaté ce partage n'a pas joué comme annoncé.

Les États qui ont produit savent innover et en se dotant d'une recherche fondamentale et appliquée apprennent à innover.

Il en résulte que nous pouvons finir par n'être que des consommateurs de produits numériques si nous n'y prenons garde, prisonniers des concepts (parfois contraires aux libertés telles que nous les défendons) et des outils faits ailleurs.

Dans ce contexte se pose la question de la façon dont la France et l'Europe peuvent réagir. La question de l'entente globale des 27 pour faire face à ce défi est de toute actualité. Il faudrait investir en amont et faire grandir des entreprises à 100% européennes pour se substituer aux acteurs comme les GAFAM et protéger, entre autres, les données des citoyens.

D'une part au plan interne, il est nécessaire que des engagements soient pris dans le domaine de la recherche, de la constitution de « clusters », comme on dit, réunissant

laboratoires publics et privés, entreprises innovantes mais aussi utilisateurs.

D'autre part au plan européen, cette souveraineté numérique doit l'objet d'une coopération à l'échelle européenne. Il existe des instances variées, des appels à projets et des financements dédiés qui doivent permettre de concrétiser les prémisses de ce réveil.

Des valeurs démocratiques à promouvoir, un contrôle à organiser

L'enjeu est de s'organiser autour des valeurs que les États membres de l'Union Européenne défendent et de répondre « groupés » via le droit européen et via la capacité à choisir des technologies et des entreprises dans lesquelles nous avons confiance et qui respectent la réglementation européenne plus protectrice.

Les entreprises spécialisées même si elles respectent la loi, doivent aussi rendre des comptes pour les actes permis par leur technologie.

Le risque est présent de voir utiliser des données sensibles et stratégiques par d'autres États ou à d'autres titres que ceux affichés.

Pour ne prendre que cet exemple, de nombreux acteurs de la santé français utilisent des outils dépendant de GAFAM ; ces données font l'objet de traitements extraterritoriaux sur lesquels la France n'a pas de prise alors qu'il s'agit de données sensibles en lien avec la santé. Ce sujet est sensible. La CNIL a

rendu un avis dans une affaire et l'État français doit réfléchir au transfert vers d'autres solutions.

J'ai pris à dessein un autre exemple car il me permet de faire trois observations.

La question de la souveraineté numérique suppose qu'elle ne reste pas un sujet de spécialistes mais aussi que la presse, les journalistes, les laboratoires indépendants ou les organisations non gouvernementales puissent en rendre compte et fassent partager leurs interrogations, leurs suggestions et leurs analyses au grand public.

Il faut plus de transparence. Alors même que la data est au cœur de notre monde, sa gestion, sa conservation, sa commercialisation restent du domaine de l'occulte trop souvent.

Il faut aussi envisager un observatoire de la donnée stratégique, publique et privée, qui scrute ce qui se passe, qui soit capable de mettre en garde et que le Parlement Français développe un « horizon scanning » sur ces sujets et qu'avec d'autres parlements nationaux de l'UE, il puisse travailler le sujet, contrôler et proposer.

Traiter un à un les grands sujets

Il y a de nombreux sujets qu'a identifiés la mission sur la souveraineté numérique.

- La question du rachat par des entreprises internationales d'entreprises stratégiques dans les domaines du numérique ou des technologies de pointes y compris utilisant des matières et composants rares ;

- La question des brevets et des licences où, semble-t-il, des entreprises innovantes se font concurrencer leurs inventions par des grands du secteur qui ont les moyens de contrer leurs actions en justice jusqu'à les « mettre à genoux « ;
- La question du soutien aux entreprises européennes des secteurs de l'intelligence artificielle, du cloud, du développement des réseaux et câblages.

Le moment de crise que nous vivons constitue ainsi une opportunité pour réfléchir à la définition de ce que sont les secteurs, produits, composants stratégiques pour l'Union européenne. Cela doit amener à ce qu'on redéfinisse les règles d'investissements dans l'UE avec 2 guidances

: 1) la sécurité au sens large de l'UE

et

2) la réciprocité du pays investisseur (création de Joint Venture avec par exemple un acteur européen avec un pourcentage minimum de détention supérieur à 51%, et / ou l' interdiction d'opérer dans des secteurs stratégiques.

Tout cela doit être sur la table.

Faire croître nos ressources

Nos ressources existent et doivent être développées au travers d'une double approche, nationale et européenne.

Il y a une fragmentation du marché européen du numérique face à des acteurs économiques tellement importants qu'ils en deviennent, comme on dit, « systémiques ».

De plus l'Union européenne n'a pas encore de politique commerciale pro-active.

On ne doit pas négliger, c'est un euphémisme, l'outil que représente la fiscalité du numérique qui est un enjeu fondamental.

Il faut donc s'inventer (ou se réinventer) dans ces domaines.

Au plan politique, un début de réponse passe probablement par l'existence d'une coordination renforcée au niveau européen pour les technologies d'État à l'image de ce qui existe aux Etats-Unis.

Faire face par la confiance et une alliance équilibrée entre le public et le privé

À l'étranger la puissance publique, que ce soit aux États-Unis ou en Chine, soutient fortement le secteur privé (cf la défense par exemple ou même la santé) et les entreprises y sont vues comme des entreprises nationales contribuant et participant à l'effort de la puissance publique.

Au plan juridique nous devons faire progresser la réglementation avec la consolidation du droit européen et le digital services act (DSA) et de bonnes pratiques qui mixent respect des principes de liberté, de protection des données et une efficacité fondée sur la confiance des citoyens et utilisateurs.

Si la France et l'UE investissent à tous le sens du terme, intelligemment le sujet, ils feront face.

Contribution de M. Damien Conce, docteur en droit

SOUVERAINETE NUMERIQUE NATIONALE ET EUROPEENNE

« La codification de l'espace numérique comme vecteur de souveraineté nationale et européenne »

Damien Concé
Docteur en Droit

La souveraineté numérique a indéniablement un aspect capacitaire : disposer de la technologie, des matériels, du savoir-faire est essentiel.
Mais il s'agit principalement d'un choix « politique », d'un modèle assumé de société. Et seule la Loi a le pouvoir de matérialiser cet idéal. Sans la loi, et on le voit particulièrement en matière de nouvelles technologies, ce sont les « Conditions Générales d'Utilisation » qui s'appliquent. Celles qui permettent à une société privée de censurer le président en exercice de la première puissance mondiale[1] ou une victime de harcèlement, pour protéger la pudeur de ses bourreaux[2]. Sans l'existence d'un cadre légal visant le Bien Commun, nous sommes sans protection.
Certes la règle de droit n'est pas une condition suffisante pour la souveraineté mais c'est une condition essentielle.

Alors que 2021 est l'occasion de commémorer le bicentenaire de la mort de l'Empereur, les juristes ne peuvent rester indifférents à l'apport du code Napoléon, non seulement pour la France, l'Europe[3] mais aussi pour le Monde[4], et ils peuvent y trouver une source d'inspiration pour défendre les souverainetés actuelles.
En effet, le code de 1804 a - dans une période troublée et alors que la France offrait au Monde un modèle de société singulier - offert une traduction juridique pratique des droits de l'Homme qu'elle venait de proclamer et permis de donner un cadre à la révolution industrielle qui s'annonçait en France. De plus il a ordonné le chaos né de la Terreur et a constitué un outil d'influence qui participe encore à la défense de notre souveraineté[5].
Il y a une analogie entre notre époque et celle de la publication du Code Civil.
Car aujourd'hui, en matière numérique, la France et l'Europe se trouvent confrontées à deux modèles qui ne conviennent ni à leurs traditions humanistes, ni à leurs ambitions.
Il s'agit, d'une part, du modèle « autoritaire » qui considère que l'ensemble des données produites par l'économie numérique appartiennent à l'Etat[6] aux fins d'organiser et de sécuriser la société

---

[1] https://www.lemonde.fr/idees/article/2021/01/11/trump-banni-de-twitter-et-facebook-les-reseaux-sociaux-entre-laxisme-et-censure_6065866_3232.html
[2] https://www.lefigaro.fr/actualite-france/mila-suspendue-de-twitter-pour-harcelement-20210315
[3] « Le Code civil français et son influence en Europe », Revue internationale de droit comparé Année 1950 2-4 pp. 757-765 : https://www.persee.fr/doc/ridc_0035-3337_1950_num_2_4_6015
[4] « L'exportation du code civil », Michel Grimaldi, in Pouvoirs 2003/4 (n° 107), pages 80 à 96 : https://www.cairn.info/revue-pouvoirs-2003-4-page-80.htm
[5] https://www.lesechos.fr/2000/02/le-droit-du-monde-ne-sera-pas-unique-1050155
[6] https://www.meta-media.fr/2019/06/20/china-big-data-les-donnees-au-coeur-dun-communisme-capitaliste-high-tech.html

(crédit social[7]…) et d'autre part, le modèle des « Majors » (GAFAM/NATU…), pour lequel la donnée est une information qui doit rester libre et sans valeur (res nulius) pour être accaparée par celui qui la transforme.

La consécration des Droits Numériques de l'Homme comme élément de souveraineté.

Comme lors de l'avènement de la révolution industrielle et du déploiement de la codification napoléonienne, la révolution induite par la numérisation de l'économie et les technologies de registres distribués initient un mouvement de destruction créatrice[8], génèrent de nouvelles formes d'asservissements[9], suscitent l'aspiration à de nouveaux droits[10] tout en permettra l'avènement d'une nouvelle économie.

En effet, il est vraisemblable que la numérisation de l'économie et l'application de l'intelligence artificielle aux activités humaines détruisent plus de « métiers » qu'elles n'en créeront[11]. Or si la matière première de l'économie de demain est la donnée et que chaque personne crée de la data par sa seule existence dans le monde sensible (dont l'empreinte est recueillie par les capteurs installés dans son environnement) ou dans l'espace numérique, il n'y a pas lieu de déposséder le producteur de la richesse qu'il génère et le concept de travail/production/création de valeur ne pourra que « muter ».

Bien sûr, l'Europe a déjà créé un lien entre la personne juridique et la donnée en consacrant le principe d'autodétermination informationnelle (accès, rectification, limitation, opposition) et en posant celui du « consentement » dans le Règlement Général (UE) 2016/679 du 27 avril 2016 relatif à la protection des données à caractère personnel (RGPD), mais cela ne peut être considéré comme suffisant au vue de l'impact de l'appropriation des datas sur la vie politique (Cambridge Analytica[12]), économique ou sociale[13].

Il convient donc de changer de paradigme, et de quitter l'ancien régime centré autour du point de vue de l'utilisateur/récepteur pour adopter celui, révolutionnaire, de l'émetteur/créateur et de créer un régime spécifique de « droit de la personnalité numérique » qui reconnaisse la propriété des données à celui qui la génère afin de donner un moyen aux citoyens de garantir leurs « libertés publiques » en saisissant les tribunaux de droit commun.
Car la première souveraineté, c'est celle des citoyens pour lesquels la première des libertés - lorsqu'ils vivent sur leur territoire national - c'est de n'être soumis qu'aux lois votées par leur représentants et jugés par leurs tribunaux, en leur nom. Ne pas leur offrir cette protection, accepter

[7] https://www.lemonde.fr/idees/article/2020/01/16/le-credit-social-les-devoirs-avant-les-droits_6026047_3232.html
[8] https://lejournal.cnrs.fr/billets/en-finir-avec-la-destruction-creatrice
[9] https://numericafrique.org/reseaux-sociaux-servissement-ou-asservissement/
[10] https://www.conseil-etat.fr/actualites/actualites/droit-a-l-oubli-le-conseil-d-etat-donne-le-mode-d-emploi
[11] https://lejournal.cnrs.fr/articles/six-scenarios-dun-monde-sans-travail
[12] https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/
[13] http://theconversation.com/comment-le-big-data-bouleverse-la-gestion-des-ressources-humaines-109214

que leur soient appliquées les règles extraterritoriales (CLOUD Act[14] …) d'autres nations, c'est la pire des atteintes à la souveraineté, celle qui peut délégitimer un Etat.

Créer un régime de « droit de la personnalité numérique » c'est aussi le moyen de rendre plus efficace et plus juste le moteur de la révolution industrielle numérique.
En effet, il est commun de dire que la data est le pétrole de l'économie numérique et que ses modes de commercialisation seront les flux économiques de demain. L'analogie est pourtant erronée, car il n'existe pas de gisement de données « pré existant ». Plus qu'un processus minier il s'agit d'un processus « agro-industriel » qui réunit : ceux qui génèrent la donnée, ceux qui la collectent, ceux qui la transforment, ceux qui la consomment. Or, pour pouvoir rémunérer l'ensemble de la chaine de valeur il faut reconnaitre le droit de « propriété » de chaque maillon.

« Payer » chaque personne pour les traces qu'elle laisse dans l'univers numérique c'est rémunérer sa production de la « matière première » de l'économie numérique. Cela impliquerait de dissiper la chimère de la gratuité et de rendre apparent le coût de chaque service, car comme disaient les américains dans les années 30, « *there ain't such thing as a free lunch*[15] ».
Ce serait aussi constituer une alternative aux projets de « Revenus Universels » que crée la crainte des disparitions massives d'emplois à la suite des nouvelles révolutions industrielles.
Ce serait enfin trouver des chemins de valorisation des actifs numériques des entités publiques (municipalités, sécurité sociale, structures sanitaires …) et ainsi participer à la réduction de leurs déficits, voir assurer le financement de leur développement.

Maitriser les effets de la révolution décentralisatrice en cours

La décentralisation portée par la révolution numérique commence déjà à bouleverser la sphère économique (crypto-monnaies[16]), et les contraintes qu'elle exerce sur les organisations traditionnelles deviennent manifestes[17].

Avec la création des Technologies de Registres Distribués (Blockchain), le principe d'organisation sociale formulé par Montesquieu, évoqué par Napoléon et De Gaulle[18] : « *si délibérer est le fait de plusieurs, décider est le fait d'un seul* » est renversé. Ce concept, qui a jusqu'à présent constitué la colonne vertébrale des organisations occidentales et justifié une efficacité fondée sur la discipline et la hiérarchie, semble devenir obsolète.

---

[14] https://www.usine-digitale.fr/article/le-cloud-act-un-texte-securitaire-americain-qui-inquiete.N800995
[15] https://www.phrases.org.uk/meanings/tanstaafl.html
[16] https://www.lemonde.fr/idees/article/2017/11/10/les-cryptomonnaies-bouleversent-l-ordre-etabli_5213131_3232.html
[17] From Bitcoin to Decentralized Autonomous Corporations Extending the Application Scope of Decentralized Peer-to-Peer Networks and Blockchains Kalliopi N. Kypriotaki, Efpraxia D. Zamani and George M. Giaglis Department of Management Science and Technology, Athens University of Economics and Business, Patission 76, 104 34 Athens, Greece
[18] «*Si délibérer est le fait de plusieurs, agir ou décider est le plaisir d'un seul.*» Montesquieu ; « *Prenez le temps de délibérer, mais lorsque le moment d'agir est arrivé, arrêtez de penser et allez-y* » Napoléon Bonaparte ; «*Si délibérer est le fait de plusieurs, agir est le fait d'un seul.*» «De la guerre», conférence écrite en 1917 et publiée dans le premier tome des «Lettres, notes et carnets» (Plon), Charles de Gaulle, page 473 ;

Les Technologies de Registres Distribués (DLT) permettent des systèmes de « gouvernance » dans lesquelles il n'y a plus de chef, mais un consensus d'acteurs égaux entre eux ; les moyens sont mutualisés, libérables en fonction des résultats et titrisables (donc liquides) et la mission est une déclaration d'intention (whitepaper).

L'ensemble vise à apporter plus de sécurité aux membres du réseau et permettre une meilleure efficacité de l'organisation que les formes traditionnelles en supprimant les intermédiaires, en réduisant les délais de réaction, et en assurant la totale transparence des processus décisionnaires, le tout avec un « cout transactionnel » extrêmement faible ….

Le réseau numérique réalise ainsi le rêve de Proudhon[19]: *« L'ordre sans le pouvoir ».*

L'image du « banc de poissons[20] », s'impose alors pour décrire les nouvelles formes sociales que cette « gouvernance » originale permet de créer.

De plus, cette gouvernance « numérique », génératrice d'une nouvelle économie, se joue des frontières, des genres et des natures (humaines, personnes morales, algorithme, intelligence artificielle…) car elle peut toutes les associer ou toutes s'en affranchir.

Cela constitue un défi que les Etats doivent appréhender pour maintenir leurs souverainetés et éviter leur obsolescence. Cela est vital pour eux, car aucune révolution technologique n'a été sans effet politique et social. Et les formes de démocratie libérale que nous connaissons aujourd'hui pourraient s'effacer devant de nouveaux modèles.

Finalement, le seul moyen pour un Etat, dans sa forme actuelle, de ne pas subir une disruption technologique qui serait une atteinte mortelle à sa souveraineté voir à son existence serait, sans doute, d'apprivoiser les effets de la révolution décentralisatrice en cours en lui accordant un statut légal.

Un code numérique

Si la Représentation Nationale devait se saisir d'un tel sujet, elle pourrait choisir de formuler une vision singulière du monde numérique fondée sur nos traditions humanistes, politiques et économiques afin de ne laisser ni la sphère privée, ni des mécanismes d'extraterritorialité porter atteinte à la Souveraineté Nationale et lui imposer sa future forme d'existence.
Elle pourrait placer le curseur en matière de droits civils numériques, de partage de la valeur des données, de protection et d'incitation au développement de l'économie numérique.
Cela permettrait en outre à la France de réellement prendre position dans la compétition mondiale, d'attirer les meilleurs projets et talents, et enfin d'exploiter au mieux nos ressources et infrastructures nationales.
C'est au législateur de dessiner le cadre juridique qui permettra à notre société d'appréhender les mutations à venir, d'offrir la sécurité nécessaire à l'épanouissement d'une nouvelle économie numérique intégrant les technologies de registres distribués, l'intelligence artificielle et offrant un cadre au déploiement des villes intelligentes.

---

[19] Pierre-Joseph Proudhon L'Anarchie sans le désordre, Thibault Isabel, Editions Autrement, mai 2017
[20] https://www.larecherche.fr/la-danse-organis%C3%A9e-des-bancs-de-poissons

A cet effet, un « Code Numérique », plus qu'une loi sectorielle, est la solution. Par l'emphase qu'il donne à la vision qui y est développée et le retentissement que l'initiative ne manquera pas de produire.
Aussi, un tel code ne pourrait pas être la simple compilation des textes déjà existants (RGPD, Signature électronique, …), au contraire il devrait être un véritable monument politique, un projet de société.
Il s'agirait de renouer avec la tradition des grandes codifications créatrices, le sujet et l'occasion s'y prêtent.

Un tel code pourrait utilement s'organiser autour des thèmes liés à la « Personnalité numérique » (1), à ceux concernant « Les institutions, professions réglementées et activités réglementées » de ce nouvel écosystème (2), et aux « Objets numériques » et « Activités spécifiques » qui en constitueront les principaux moteurs (3) ;

1. La Personnalité Numérique

Dans le concert des nations et pour protéger la souveraineté des peuples européens, de la France voir de l'Europe, l'élément le plus symbolique, mais paradoxalement aussi le plus efficace, serait de consacrer la notion de « Personnalité Numérique ».
En effet, c'est sur cette base légale de protection des personnes que pourront se régler juridiquement et pacifiquement la confrontation internationale autour de l'accès aux données.

Reconnaitre une « personnalité numérique » c'est tout d'abord établir que celle-ci est un attribut de la personnalité juridique des personnes physiques et morales.
C'est aussi distinguer la personnalité numérique de l'individu numérique (anonymisation de la personnalité juridique) pour forger les concepts permettant d'établir un régime économique qui n'entraine pas une réification de la personne humaine voir une réduction des populations en esclavage numérique.
Il en découlerait que les données de la «personnalité numérique » seraient des biens « hors du commerce » et ceux de l'individu numérique seraient des biens « du commerce » en référence aux règles civiles de droit commun.

Etablir une « personnalité numérique » imposerait d'en définir les attributs.
Ceux-ci pourraient consister en différents droits, chacun disposant de ses propres limites (l'ordre public, la sécurité commune…) :

- **Le droit à l'accès à la sphère numérique** qui comprend le droit à la connexion au réseau, le droit à la neutralité du réseau, le droit au compte numérique ou au portefeuille numérique (wallet) ;
- **Le droit à l'anonymat et à la cryptographie** qui comprend le droit à l'anonymat et au pseudonyme, le droit d'usage de la cryptographe dans les limites posées par la protection de l'intérêt général, et le droit au contrôle des données personnelles ;
- **Le droit à l'oubli ;**

- **Le secret des correspondances, des adresses et des modes d'identification ;**
- **Le droit à la retranscription numérique fidèle** des attributs physiques du sujet de droit et la protection contre les atteintes à la personnalité numérique (cf deepfake)…

Il conviendrait aussi d'établir les moyens de protection de la personnalité numérique pour rendre effectifs ces droits.
Le premier moyen pourrait consister à permettre aux personnes juridiques de revendiquer la propriété de l'ensemble des données générées par leur personnalité numérique et de leur reconnaitre un « droit moral » sur celle-ci.
Par analogie au droit d'auteur il conviendrait aussi d'établir que les personnes juridiques disposent de droits pécuniaires sur ces données, dans la limite de la commercialité de ces biens.

Ainsi, chaque personne juridique, aurait droit à une juste rémunération automatique pour la collecte et l'usage des données numériques qu'elle génère.

Par ailleurs, reconnaitre une valeur patrimoniale aux données permet de faire application des règles de droit commun en matière de minorité, d'incapacité ou d'empêchement, de liquidation des personnes physiques ou morales.
Il serait aussi pertinent, de prévoir la possibilité de nommer un exécuteur testamentaire pour procéder au nettoyage de l'empreinte numérique du défunt et permettre la dévolution successorale de ses droits pécuniaires.

Une telle partie du Code numérique pourrait aussi être l'occasion d'accorder la personnalité juridique aux entités autonomes décentralisées (DAO) et de distinguer entre personnalité juridique et capacité juridique pour ce qui concerne non seulement les organisations autonomes décentralisées (DAO) mais aussi les intelligences artificielles (IA).
C'est cette partie qui permettrait à l'Etat d'appréhender les effets de la révolution de la décentralisation. Et par exemple, anticiper ce que pourrait être la réponse pénale réprimant les comportements criminels ou frauduleux d'Organisations Autonomes Décentralisées[21] ou d'intelligences artificielles autonomes décentralisée…

Enfin cette première partie pourrait rassembler et donner une cohérence aux textes déjà publiés à propos de l'identité et de la signature numérique.

2. Les institutions, professions réglementées et activités réglementées

Une seconde partie du Code pourrait être dédiée à l'organisation de l'écosystème permettant le développement harmonieux et le contrôle de l'économie numérique décentralisée.

[21] https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/

Créer des Institutions souveraines

Afin de distinguer entre ce qui relève de la Loi et ce qui relève du domaine réglementaire, une première étape consisterait à créer une Autorité Nationale Numérique, à l'image de ce qui a été créé à Malte pour accorder les agréments, exercer le contrôle, prendre les mesures de police administrative, assurer la formation et contrôler la formation des professions dépendants de son autorité. Cette Autorité disposerait d'un pouvoir disciplinaire et organiserait les professions réglementées d'avoués digitaux, de certificateurs techniques et d'agents de change numériques.

Le code pourrait aussi créer une **Bourse Souveraine de Souscription et d'Echange d'Actifs Numériques** (Exchange) et un **Dépositaire Souverain d'Actif Digitaux** (Custodian). En effet, les « Exchanges », plateformes boursières numériques privées, connaissent aujourd'hui les mêmes affres que connaissent les bourses traditionnelles depuis le XVIIIème siècle[22] : fausse nouvelle, manipulation de cours[23] …
Par ailleurs les dépositaires (Custodians) se font « hacker » avec la régularité des attaques de diligences dans les westerns[24].
En conséquence, le système financier traditionnel est très réticent à permettre les transferts de fonds « fiat » entre les « exchanges » et les comptes bancaires traditionnels.
En outre, il doute (non sans arrières pensées) de l'effectivité des contrôles KYC, AML effectués par ces nouveaux opérateurs[25].

Aussi, l'établissement d'une certaine sécurité et confiance sera essentielle si l'on souhaite raccorder la nouvelle économie numérique au système bancaire, financier, économique traditionnel.
Pour cela, et c'est un comble pour des protocoles blockchain fondés sur l'absence de « tiers de confiance », il faut justement un « acteur de confiance » disposant des moyens de contrôle, d'une capacité d'auto-assurance (vu que peu « d'exchanges » sont assurés[26]), et d'une certitude de permanence dans le temps.
En tout cas, jusqu'à ce que le marché ait atteint une certaine maturité.
Or, le seul acteur disposant de ces caractéristiques, c'est l'Etat. Et il en va de même pour les « Custodians » (Dépositaires), pour lesquels les Etats développés sont les rares entités à disposer des compétences, des moyens de cyber sécurité et d'auto-assurance.

Créer ces « Exchanges Souverain » et « Custodians Souverain » est donc le moyen de générer l'osmose entre le système bancaire et financier traditionnel et cette nouvelle économie qui peut

---

[22] https://www.persee.fr/doc/ecofi_0987-3368_1998_num_47_3_2661
[23] https://journalducoin.com/exchanges/trading-crypto-les-exchanges-manipulent-ils-les-volumes/
https://medium.com/@marvinneuefeind/manipulations-in-the-cryptosphere-8665f2e06c57
https://journalducoin.com/exchanges/manipulation-des-volumes-dechanges-par-bitforex-coinmarketcap-complice/
[24] https://cointelegraph.com/news/hackers-withdraw-7-000-bitcoins-in-binance-crypto-exchange-security-breach?utm_source=Telegram&utm_medium=social
https://blockonomi.com/trade-io-hacked/
[25] https://www.coindesk.com/most-crypto-exchanges-still-dont-have-clear-kyc-policies-report
[26] https://flagshipcrypto.com/which-cryptocurrency-exchanges-are-insured/

créer la richesse dont ont besoin nos sociétés pour renforcer leurs modèles sociaux tout en apportant des réponses pertinentes aux enjeux de souveraineté numérique auxquels font face les états modernes.

De plus, cela ne serait pas réellement une charge pour le Budget de l'Etat puisque l'ensemble de ces services devrait générer des rémunérations (frais de transaction, droits de garde…) couvrant leur coût de fonctionnement.

Constituer des Professions Réglementés

Sur la base de cet écosystème trois types de professions réglementées pourraient être crées afin de civiliser l'activité économique numérique sauvage : les **Avoués numériques**, les **Certificateurs Techniques** et la profession réglementé d'**Agents de Change auprès de la Bourse Souveraine de Souscription et d'Echange d'Actifs Numériques et des Bourses Privées de Souscription et d'Echange d'Actifs Numériques**.

C'est la voie qu'a choisi partiellement Malte pour demeurer « agile ». Cet état européen, réellement précurseur, a choisi de s'appuyer sur le secteur privé pour s'assurer que la pratique de la technologie des registres distribués respecterait les critères qualitatifs posés par la puissance publique. La confiance n'excluant pas le contrôle, elle a choisi de créer de nouvelles « professions réglementées », soumises à son contrôle et justifiant de compétences techniques spécifiques, pour effectuer ces tâches. Cette solution est particulièrement efficace, en terme opérationnel, de finances publiques, de création d'emplois et devrait être une source d'inspiration.

Ainsi les *Avoués digitaux*, s'assuraient que les projets et opérations « numériques » seraient conduits dans le respect des règles applicables et les « *Certificateurs Techniques* », valideraient la conformité aux standards des procédures techniques et certifieraient la juste transcription des engagements pris par les parties dans les algorithmes. Cela afin d' assurer la prophylaxie de l'écosystème.
En effet, ce n'est pas parce que la « blockchain » est supposée être « trustless[27] » qu'il ne convient pas de valider préalablement (i) que les informations mises dans les blocks sont « correctes » et (ii) que le fonctionnement du protocole et des smart contracts est bien conforme aux engagements pris par les promoteurs dans le cadre des lois applicables.

A ces deux professions, existant déjà dans la régulation maltaise, il conviendrait d'ajouter celle « *d'Agent de Change* ». En effet, toujours dans le but d'alléger les contraintes reposant sur les institutions publiques, il serait pertinent de confier à des « Portier » (Door Keeper) le soin de vérifier l'honorabilité des usagers et la provenance des fonds ainsi que le recommande déjà le GAFI[28].

[27] https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6
[28] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

Distinguer les activités libres, les activités numériques réglementées et les activités agréées

Les activités économiques ont besoin de règles pour prospérer, mais il s'agit aussi de délimiter strictement les contours d'un droit spécial exonératoire des règles de droit commun (démarchage financier, conseil en investissement, droit de la consommation, monopole monétaire…) permettant d'assurer la liberté et la sécurité nécessaire au développement de nouveaux acteurs économiques.

Une fois ceci posé, il conviendrait de distinguer entre des activités numériques réglementées, des activités agréées et les activités libres.
A titre d'exemple, les premières pourraient réunir la « *Promotion, la souscription et la vente de produits digitaux* » (promotion, lancement et souscription d'ICOs, actes de commerces relatifs à des jetons où crypto monnaies…), les « *Opérateurs de plateformes et de services de Technologie de Registres Distribués* » (Exchange / Custodian privés), les « *Conseils en Produits Digitaux* » (Advisors, Conseils en Investissement…) et les « *Sociétés de Gestion de Produits Digitaux* » (Fonds d'investissement en token / cryptos ; trading…)… ;

Il conviendrait surtout, dans cette partie, de rendre effectif le droit aux comptes bancaires et aux assurances professionnelles pour les professions réglementées et les titulaires d'une autorisation d'exercer une activité réglementée ou agréée.
Un mécanisme comparable à celui mis en œuvre au profit des « interdits bancaires », avec désignation par la Banque de France d'une Banque Dépositaire (Caisse des Dépôts ?) pourrait être envisagé.

3. Les objets numériques & activités spécifiques

La troisième partie du Code pourrait être consacrée au régime juridique des principaux objets de cet écosystème tels que : les différentes technologies de registres distribués, les jetons (Tokens), les cryptomonnaies et les contrats auto-exécutés (smart contracts), mais aussi à certains cas d'usages spécifiques tels les Smartcities et l'usage de la blockchain dans des procédures administratives et pour la valorisation des actifs numériques des entités publiques.

Pour ce qui est du régime juridique des *Technologies de Registres distribués*, il s'agirait tout d'abord de définir la nature juridique des Blockchains publiques / privées mais aussi celle des technologies permissionnées (ex. blockchain permissionnées de consortium[29]).
Une typologie d'opérateurs pourrait être établie et la responsabilité de chaque opérateur pourrait être définie. Ce serait l'occasion de déterminer les différents types d'opérateurs agréés (ex. centres d'hébergement des données, oracles, contrôleurs, administrateurs).
Puis il conviendrait de définir la valeur probatoire attachée aux informations contenues dans la blockchain. Celle-ci pourrait dépendre de la nature de la blockchain considérée mais aussi du degré

[29] https://www.researchgate.net/publication/328887130_Consortium_Blockchains_Overview_Applications_and_Challenges

de contrôle de la donnée inscrite dans la blockchain (Oracle). Cette valeur probatoire pourrait donc varier entre le « *commencement de preuve par écrit*[30] » et la « *présomption mixte*[31] ».

Ainsi, le « *Jeton* », qui est au cœur de cette nouvelle économie devrait pouvoir être défini comme la « titrisation » d'un bien, d'un droit ou d'un service et être rattaché à la notion de bien meuble incorporel.
Sa fongibilité et sa négociabilité devrait aussi être considérées. Et lorsqu'il serait fongible et librement négociable, il devrait être qualifié de valeur mobilière disposant d'un statut spécifique dérogatoire du droit commun financier.
La qualification juridique du jeton serait l'occasion de distinguer les jetons numériques, des supports monétaires numériques, des instruments financiers numériques ou encore des portefeuilles numériques.

Enfin, les *contrats auto exécutés* (smart contracts) pourraient être qualifiés de contrats d'adhésion[32]. Et le code pourrait prévoir leurs conditions de validité et par là même, les critères de leur homologation préalable. Ainsi, il pourrait, par exemple, être précisé que les contrats auto-exécutés doivent être la transcription numérique fidèle d'un « contrat Maître » écrit (littéraire) et homologué par l'autorité compétente. Ce « contrat Maître » pouvant alors faire l'objet de contentieux devant les juridictions de droit commun.
Pour être homologué, ce contrat ne devrait pas comporter de clauses abusives, ni de dispositions léonines et se référer à des « modèles[33] » validés par l'autorité compétente. Selon la matière ou le cas d'usage, ledit contrat pourrait aussi devoir comporter les dispositions permettant de rendre effectif la protection de la personnalité numérique[34] (RGPD) par application de modalités d'anonymisation validées conjointement par l'Autorité Nationale Numérique, l'ANSSI et la CNIL.

Une dernière partie du Code pourrait être consacrées aux activités spécifiques qui seront véritablement les moteurs économiques de demain.

Ainsi le code pourrait donner un cadre juridique aux smartcities afin de s'assurer que celles-ci ne seront pas soumise aux normes privées et ou aux conditions générales d'utilisation de leurs fournisseurs, voir à des standards non respectueux des valeurs européennes.
Légiférer sur les smarcities, participerait donc au renforcement de la souveraineté à la fois des territoires et de la Nation.
Dans ce cadre, il pourrait être organisé l'usage de technologies de registres distribués permissionnées de consortium pour la création de « métropoles connectées intelligentes »(Samrtcities) sur le territoire national.

---

[30] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438450
[31] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000032042336
[32] https://policyreview.info/articles/analysis/standard-form-contracts-and-smart-contract-future
[33] https://arxiv.org/abs/1608.00771
[34] https://civis-blockchain.github.io/

Ces projets devraient recourir à des serveurs et des clouds situés exclusivement sur le territoire national ou de l'union européenne et être organisés en cohortes d'usagers, de prestataires, de services administratifs et d'entités de contrôle bénéficiant d'un agrément.
En outre, l'architecture de ces smartcities devrait comprendre des Oracles chargés d'anonymiser la data gérée par la smartcity ainsi que des organes dédiés à la cybersécurité de la « métropole connectée intelligente ».
Le code pourrait aussi imposer que les fonctions d'administrateur et de délégué à la protection des données soient assumées par un service public métropolitain dépendant directement d'une autorité élue pour garantir le coté démocratiques de ces nouvelles institutions.
Enfin, le code devrait prévoir que la création, le développement et la gestion des projets de Métropole Connectée Intelligente, ne pourront se faire que par émission de jetons dans le cadre de la Bourse Souveraine de Souscription et d'Echange d'Actifs Numériques.
Que ceux-ci devant en outre faire l'objet d'un dépôt auprès du Dépositaire Souverain d'Actif Digitaux. Le Code devrait enfin imposer que les fonds en monnaie fiduciaire échangés contre les jetons émis par les smartcities fassent l'objet d'un dépôt auprès de la Banque de France

Par ailleurs, le code pourrait établir un cadre d'usage de la technologie blockchain et des « smart contacts » dans les relations entre les autorités publiques et les acteurs privés.
Ce cadre pourrait s'appliquer aux appels d'offres, contrats publics privés ainsi qu'à toutes les opérations de subventions.

En effet le mécanisme des Initial Coin Offering (ICO) permet à un porteur de projet (émetteur) de préfinancer la création de son projet en émettant des « jetons » qui sont souscrit par le marché. Lorsque le souscripteur d'un jeton paie le prix de ce jeton en « fiat » ou « cryptomonnaie », au moment de son émission, le prix de vente est séquestré entre les mains d'un « dépositaire ». Chaque fois que le projet de l'émetteur passe des étapes convenues d'avance et que ces franchissements sont constatés (exemple, émission d'un K-bis, production d'une expertise…), une partie des sommes séquestrées sont livrées par le dépositaire entre les mains de l'émetteur, automatiquement par le jeu du « smart contract ». Donc si les marchés publics ou les subventions étaient gérées sous la forme d'ICO présentée par une Emetteur privé et souscrites par les administrations concernées, on peut imaginer les gains de productivité, d'efficacité, de transparence et donc « in fine » de croissance que cela pourrait produire.

Ce cadre pourrait aussi permettre de valoriser les actifs numériques des autorités publiques (données géographiques, données d'usage, données médicales, …) en assurant leur anonymisation selon une architecture semblable à celle établie pour les smartcities.

A titre d'exemple les données de santé de la population française sont essentielles à la recherche moderne. Or, aujourd'hui elles ne sont ni exploitables par les chercheurs européens ni commercialisables par les hôpitaux, la Sécurité Sociale, la Caisse Nationale d'Assurance Maladie ou les patients. Si demain, le code évoqué dans ces lignes était en vigueur, on pourrait imaginer que : les données de santé (résultats d'examens, antécédents médicaux …) soient collectées par un « Oracle » qui les anonymise et les encrypte. A ce stade le lien étant rompu entre la « personnalité

numérique » et l'individu numérique, lesdites données feraient partie des « biens du commerce ». Chacune de ces données serait entrée dans la blockchain « souveraine » de consortium.
Les startups médicales, les groupes de l'industrie pharmaceutique, les actuaires, les professionnels du Big Data… et tout autre professionnel qui souhaiterait avoir accès à ce « lac de données[35] » pourrait alors le faire moyennant le paiement d'un prix.
Ce prix serait payé en « jeton » acquis sur la Bourse souveraine en échange de Fiat.
Ce prix, payé pour l'accès au « lac de données » et pour chaque usage des données qu'il contient, serait immédiatement réparti entre chacun des intervenants (Sécurité Sociale, médecins ou hôpitaux ayant effectué les analyses … patient) grâce à l'application automatique de la clé de répartition figurant dans le « smart contract ».
Ainsi, dès demain, le système de santé français pourrait trouver d'autres sources de financement que la solidarité nationale tout en respectant les droits des citoyens.

En conclusion, si la crise sanitaire a démontré les fragilités de nos sociétés européennes, elle a été aussi l'occasion de remettre à l'honneur le terme de souveraineté et de nous forcer à effectuer la revue de détail de nos forces collectives et de nos failles structurelles.
Cette revue a fait apparaitre que le secteur numérique est non seulement une source de crise de souveraineté mais peut aussi être à l'origine d'opportunités[36].
L'étymologie du terme « crise » renvoi au grec Krisis qui signifie « décision » et cela nous permet de souligner qu'il appartient aujourd'hui à la Représentation Nationale de choisir entre deux scénarii :

- Soit la France et l'Europe succomberont à un modèle étranger ; accepteront que leurs datas soient captées par des acteurs non européens au prix de concessions illusoires ; que leurs standards techniques soient déterminés par d'autres, que leurs souverainetés soient minées par de nouvelles structures sociales qu'elles ne sauront appréhender (…) ; passeront à côté des opportunités de l'économie numérique (ex les Exchanges et le marché des actifs virtuels)…

- Soit le Législateur français assumera sa responsabilité historique de créer le régime des « Droits Numériques de l'Homme » et de dessiner un régime juridique des technologies de registres distribués au sein d'un Code Numérique. Cela d'entrainerait l'Europe dans une dynamique protégeant les droits des citoyens européens, permettant l'épanouissement d'une économie numérique correspondant aux valeurs de la France et de l'UE et d'offrir un modèle aux pays dont la tradition ne se reconnait ni dans les modèles autoritaires ni dans ceux des « Majors ».

[35] https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1165409-data-lake-ou-lac-de-donnees-la-solution-reine-du-big-data/
[36] https://www.sorbonne-universite.fr/parutions/la-souveranete-numerique-dans-lapres-crise

Contribution de Scaleway

Scaleway
The cloud that makes sense

Mission d'information de l'Assemblée Nationale "bâtir et promouvoir une souveraineté numérique nationale et européenne"

****Contribution de Scaleway****

Scaleway: qui sommes-nous?

Scaleway est une ETI française basée à Paris, filiale du groupe Iliad - côté à l'Euronext Paris (ILD.PA). Notre entreprise est l'un des leaders européens dans le domaine du cloud. Nous sommes parmi les rares acteurs en France et en Europe à posséder une maîtrise d'ouvrage et sans dépendances à trois niveaux:

- Conception et opération de data centers sur le territoire français, extrêmement performants sur le plan énergétique
- Infrastructure matérielle (fourniture de puissance de calcul et de stockage)
- Infrastructure logicielle (Iaas et PaaS)

Nous comptons 350 salariés entre Paris et Lille, et avons réalisé un chiffre d'affaires d'environ 80 millions d'euros en 2020. Nous déployons des services via six data centers situés en région parisienne, à Amsterdam et Varsovie, et comptons 300 000 clients professionnels dans plus de 160 pays. Scaleway est également un membre fondateur de GAIA X.

Vers une "décennie du cloud" en Europe: opportunités et défis

L'accélération radicale de la transformation numérique de nos économies et de nos sociétés, sous le coup de la pandémie de COVID-19, a été le révélateur d'une dépendance collective accrue à l'égard des infrastructures cloud et des services qui en découlent. Dans le contexte de la crise sanitaire, en effet, on a pu voir à quel point la continuité et la résilience des entreprises dépendent désormais largement de la qualité de ces infrastructures et services numériques. Selon Gartner, l'accélération de l'adoption du cloud, conséquence de cette crise, est même devenue une "nouvelle normalité". Le cabinet IDC, repris dans une étude récente menée par KPMG, indique également que, de 53 Mds de dollars en 2020, les marchés du cloud devraient représenter quelque 560 Mds de dollars d'ici 2030 (poids actuel du marché des télécoms).

La fourniture de services cloud devenant la colonne vertébrale de la transformation numérique, il est indispensable de conduire sans attendre une réflexion quant à la dimension stratégique que ce secteur d'activité recouvre pour le fonctionnement de nos économies, sociétés et nations.

De fait, cette nouvelle dimension stratégique a d'énormes implications qui doivent être évaluées par le législateur français et européen, dans un contexte où :

- Très peu d'acteurs, non-européens, fournissent plus de 75 % des services cloud dans le monde (phénomène d'oligopole bien documenté).

- Les États-Unis ont probablement cinq à dix ans d'avance sur les entreprises européennes en termes d'adoption du cloud.
- Nos valeurs européennes diffèrent largement de celles des autres superpuissances, notamment en termes de protection des données, de transparence, d'interopérabilité, de contrôle des utilisateurs sur leurs données.
- Les acteurs du cloud qui dominent aujourd'hui en Europe sont soumis aux législations régissant ces superpuissances, principalement motivées par des intérêts de sécurité nationale, avec des impacts extraterritoriaux étendus démontrés (vecteurs d'une conséquente incertitude juridique) sur le sol européen. Ces législations s'appliquent aux acteurs américains présents sur le sol européen, aux acteurs européens ayant des sociétés mères américaines, ou aux données traitées/stockées sur le territoire d'un État membre de l'UE par un acteur américain. Toutefois, le manque de clarté à ce sujet rend propice la diffusion de discours potentiellement contradictoires, pouvant induire les clients en erreur.
- D'autres grandes puissances ont développé des politiques industrielles audacieuses favorisant l'adoption de solutions de fournisseurs nationaux de services cloud. Cela soulève la question de l'égalité des conditions de concurrence ("level playing field").
- Nous sommes actuellement témoins, de la part de nos concurrents non-européens, de stratégies commerciales agressives et pluriformes visant à bloquer les tentatives en cours au niveau de l'UE pour fédérer et renforcer l'écosystème européen du cloud.
- En parallèle, nous percevons avec inquiétude une stratégique de la part de ces acteurs visant à "cannibaliser" la chaîne de valeur du cloud en Europe, afin d'éviter l'émergence d'un écosystème indépendant (i.e issu de logiciels open-source ou close source d'origine privée, mais européenne), en particulier sur les segments du cloud à plus forte valeur ajoutée à terme (la couche logicielle).

La perspective de Scaleway sur la souveraineté numérique

1/ Notre philosophie: la souveraineté numérique, synonyme d'ouverture vers le monde

Pour éviter toute incompréhension quant aux propositions exposées ci-dessous et à l'état d'esprit sur des concepts volontiers sujets à controverse, il convient d'emblée de préciser que:

- l'utilisation du vocable de souveraineté, traditionnellement appliqué à un échelon territorial et politique déterminé, doit être manipulée avec prudence dans l'univers numérique. La notion de frontières n'y est effectivement pas prégnante, et les interdépendances, globales, extrêmement marquées. En particulier, nous invitons à ne pas confondre les notions de souveraineté et souverainisme - nous rejetons fermement ce dernier concept, comme en témoigne la structure de notre activité: loin de vouloir se cantonner aux marchés (publics) français, Scaleway a des ambitions européennes et mondiales. Nous réalisons d'ailleurs déjà plus de 40% de notre chiffre d'affaires à l'export.
- Il ne saurait être question d'inciter à se passer, par des mesures protectionnistes ou restrictives, de l'excellence des services fournis par un certain nombre des acteurs dominants de la tech - ce qui serait un non-sens économique, commercial et politique. Tout l'enjeu réside plutôt, via une action coordonnée à l'échelle

européenne, de mettre fin aux effets de surdomination de marché et aux excès des effets de réseau (caractéristiques de l'économie numérique) que nous observons aujourd'hui.

- En ce sens, notre vision de la souveraineté n'est pas marquée par une volonté d'exclusion ni de repli sur soi, mais bien de rééquilibrage des rapports de force. Notre objectif est de permettre à l'Europe, grâce à des politiques publiques volontaristes, de participer aux "termes de la conversation" sur la scène mondiale, dans le secteur numérique - nous donnant par là le poids requis pour protéger nos valeurs profondément européennes, humanistes et universelles.
- L'écosystème industriel européen a aujourd'hui atteint une maturité permettant aux acteurs du cloud européens de satisfaire plus de 80% des cas d'usage rencontrés sur le marché - ce qui rend réaliste un tel objectif de rééquilibrage.

2/ La confiance dans le cloud | vers une meilleure définition à l'échelle française et européenne

La récente doctrine "cloud au centre" annoncée par le gouvernement le 17 mai dernier a mis au centre des débats la notion de confiance des offres cloud commerciales, auxquelles les administrations auront par défaut recours d'ici un an, pour le déploiement de nouveaux projets informatiques.

Or, de notre point de vue, la confiance ne saurait se labelliser, en cumulant, tel que cela est proposé dans la doctrine, l'octroi du label SecNumCloud et l'examen, par une analyse juridique, de l'exposition des offres cloud à des législations extraterritoriales.

Cette définition reviendrait à exclure du champ des offres de confiance un nombre substantiel d'acteurs français qui se différencient pourtant par leur crédo souverain, au prix d'investissements conséquents.

Nous appelons donc à mieux qualifier la notion de confiance dans le cloud, qui aura vocation à être labellisée par l'ANSSI, pour que les enjeux de souveraineté et d'immunité aux lois extraterritoriales soient spécifiquement reconnus comme des facteurs de confiance par les autorités publiques - et, par effet d'entraînement, les clients des fournisseurs de cloud.

3/ Mesure de l'immunité aux lois extraterritoriales | une analyse fine s'impose pour ne pas promouvoir une "souveraineté partielle"

Si les problématiques d'actionnariat, de localisation et de propriété des data centers sont des paramètres significatifs pour évaluer l'immunité des fournisseurs de cloud à des lois non-européennes à portée extraterritoriale, il faut garder à l'esprit que le "cloud" recoupe tout autant la couche physique (data centers) que la dimension hardware et logicielle.

Ainsi, sous l'angle de la "souveraineté logicielle", souvent peu évoquée, le transfert de métadonnées (indirectement porteuses de données personnelles, car pouvant être reconstruites) hors UE, la maîtrise du code source des technologies logicielles utilisées, sont autant d'exigences à considérer. Il est également important de savoir identifier des facteurs d'ordre géopolitique (e.g: dépendance à des régimes de contrôle des exportations en matière de licences, dans des Etats tiers, cf précédent Huawei aux Etats-Unis) pour identifier en transparence les vulnérabilités auxquelles peuvent être confrontés les acteurs cloud.

Au niveau français (via un label de confiance affiné, cf *supra*) comme européen (à travers le schéma de certification de cybersécurité pour les fournisseurs de cloud, en cours d'élaboration), il est nécessaire que les autorités publiques se dotent d'une capacité d'évaluation, avec un niveau de granularité suffisant, de l'immunité aux lois extraterritoriales, depuis la dimension physique jusqu'aux composants logiciels qui constituent le cloud - sous peine de faire la promotion d'une "souveraineté partielle" auprès de l'ensemble du marché.

4/ Vers des politiques "multicloud first" | un double enjeu en terme de résilience et de liberté pour l'utilisateur

Au-delà de la dimension technologique, être un opérateur de data center et un fournisseur de cloud, cela revient à être un professionnel de la gestion de risques, sans discontinuité possible. S'il est un apprentissage que nous tirons de notre expérience et qui devrait inspirer les politiques publiques en matière de cloud, c'est que la dépendance est l'ennemie de la résilience. Cette dépendance peut-être de plusieurs ordres:

- La dépendance à l'égard d'un seul serveur ou d'un seul datacenter
- la dépendance trop importante envers quelques fournisseurs clés, dictant leurs conditions commerciales et compromettant la liberté de choix des utilisateurs - tout en cadenassant l'innovation et l'arrivée de challengers sur le marché

Or, c'est bien la promotion d'une approche multi-cloud qui permettra, à terme, d'atteindre le niveau le plus élevé de résilience possible. Cela suppose toutefois que les offreurs développent des architectures interopérables, et que la portabilité des données passent de la fiction à la réalité, tant sur un plan technique que commercial - pour casser les dynamiques d'enfermement propriétaire qui restent trop encore la norme dans les marchés, oligopolistiques, du cloud computing, au profit des acteurs dominants. Scaleway est partie prenante du code de conduite développé par l'association SWIPO sur la portabilité des données. Toutefois, cette démarche volontaire, d'autorégulation, trouve sa limite dans l'absence de volonté réelle des acteurs dominants d'y souscrire. Alors que la Commission européenne envisage, entre autres options, de développer un droit contraignant ou opposable à la portabilité des services cloud, il serait opportun que la représentation nationale approfondisse en parallèle ce sujet.

Les initiatives de la Commission européenne visant à rééquilibrer les conditions de concurrence dans la sphère numérique (digital markets act) ont également un rôle clé à jouer pour favoriser ce rééquilibrage en faveur du multi-cloud. Une vigilance particulière reste pour nous de mise quant au traitement des services cloud dans ce contexte, certains acteurs dominant appelant à retirer les services cloud du périmètre du DMA.

Apparté: GAIA-X, un accélérateur pour l'écosystème européen...Sous conditions

S'il est de plus en plus communément admis que GAIA X n'a pas vocation à être un instrument de souveraineté numérique pour l'Europe, de nombreuses attentes reposent sur le label que l'association et ses membres seront amenés à proposer dans les prochaines semaines - fondé sur les valeurs de l'UE en matière de protection des données, de sécurité, de transparence ou de réversibilité; le tout afin d'orienter de façon vertueuse l'explosion attendue de l'adoption du cloud sur notre continent, dans les prochaines années.

Ce succès est toutefois conditionné à la capacité des acteurs européens d'édicter un lot de règles et d'exigences, en ligne avec les valeurs susmentionnées. L'orientation (par des biais indirects) de la gouvernance de l'association et/ou des travaux techniques sous-jacents à ce label, au profit d'acteurs non-Européens constitue un véritable risque: que GAIA-X ne devienne un instrument permettant de renforcer encore la position dominante des acteurs traditionnels du cloud, plutôt que de mettre en valeur la diversité de nos écosystèmes numériques nationaux.

5/ L'autonomie industrielle | vecteur de souveraineté dans un monde numérique interdépendant

Dans cette perspective de rééquilibrage des rapports de force géopoliques et commerciaux dans le domaine du cloud, nous estimons qu'un dernier volet devrait porter sur le développement d'une politique industrielle, à l'échelle française et européenne, visant à stimuler la croissance des acteurs locaux, français et européens, mettant en oeuvre une une réciprocité en cas d'accès asymétrique aux marchés publics locaux.

De nombreuses études démontrent comment, aux Etats-Unis (eg: Buy American Act, Small Business Act), en Chine la passation de marchés publics est un levier favorisant massivement les acteurs locaux, déjà dominants dans le cloud - dynamiques de marchés captifs dont sont de facto exclus les challengers européens. Dans toutes les puissances (Etats-Unis, Chine, Inde, Brésil, Corée du Sud), on trouve également des réglementations en matière de localisation des données qui rendent compliquée l'application d'une concurrence libre et non-faussée entre acteurs locaux et Européens. L'Europe et son marché intérieur se trouvent donc dans une position très singulière.

À l'heure de la relance de nos économies et en réponse à de telles pratiques, les marchés publics financés par l'UE et les budgets nationaux devraient être plus que jamais utilisés comme un levier pour :

- Prioriser les fonds vers l'adoption du (multi)cloud par les entreprises européennes et la modernisation des administrations ;
- Montrer l'exemple lorsque les institutions publiques passent des marchés pour leurs propres besoins, afin de promouvoir des exigences fondées sur la transparence, l'innovation, la sécurité, la souveraineté des données et la neutralité climatique.
- Des démarches concrètes devraient aussi être menées pour graver notre "instinct d'acheter européen" dans le droit. Les acteurs de l'industrie européenne du cloud sont pour la plupart des entités de petite ou moyenne taille : lutter à armes égales avec les géants de la tech s'avère extrêmement ardu, de surcroît dans un environnement où les pratiques anticoncurrentielles sont légion.

Les infrastructures cloud recouvrant une dimension de plus en plus stratégique pour le fonctionnement de nos sociétés et de nos économies, il est urgent de placer le sujet de la non-dépendance à l'égard des technologies (hardware/software), actifs ou services cloud non européens au plus haut des priorités. La mise en œuvre d'un instrument juridique restreignant l'accès aux marchés publics pour les acteurs non européens, en cas d'accès asymétrique aux marchés publics locaux, serait un moyen concret de rééquilibrer au moins partiellement les conditions de concurrence, en générant de fortes externalités positives pour l'industrie du cloud européenne. Le tout pour conjuguer ouverture et fermeté, en cas d'entorses aux règles du libre-échange de la part de nos partenaires commerciaux.

Contribution de La Poste

Mission d'information «Bâtir et promouvoir une souveraineté numérique nationale et européenne» - contribution écrite Groupe La Poste

Le nouveau plan stratégique « La Poste 2030 – engagée pour vous », confirme notre ambition de devenir la première plateforme européenne du lien et des échanges, humaine et numérique, verte et citoyenne, au service de ses clients dans leurs projets et de la société tout entière dans ses transformations. La stratégie de transformation numérique est une des priorités de ce plan stratégique.

Historiquement, La Poste est un acteur central des échanges dans le monde physique, assurant la fiabilité des communications et l'inviolabilité des correspondances, reconnu comme tiers de confiance. Il est donc naturel pour La Poste de développer une activité similaire dans le monde numérique. Ce positionnement signifie que les solutions fournies garantissent la confidentialité des données et respectent les principes éthiques fondamentaux, dans un souci d'inclusion numérique et sociale.

Le Groupe La Poste, acteur du numérique de confiance, souhaite souligner trois points relatifs aux enjeux de souveraineté numérique.

1) La crise sanitaire a fait évoluer le rapport des entreprises au numérique

La crise sanitaire a accéléré la transformation numérique des entreprises. **Certaines entreprises qui n'avaient jusqu'alors pas encore franchi le pas de la numérisation se sont retrouvées ralenties voire bloquées** dans la réalisation de certaines de leurs activités parmi les plus courantes comme signer un document, archiver des documents ou vendre en ligne.

Le défi de la numérisation des TPE/PME est en particulier apparu comme un enjeu majeur. Les plateformes permettant aux commerçants de vendre en ligne ont alors connu un succès important. C'est le cas notamment pour notre plateforme « Ma Ville Mon Shopping ». Notre filiale Docaposte s'est engagée auprès de ces entreprises en répondant aux appels à projets de France Num sur les formations/ sensibilisations au numérique.

L'enjeu pour les fournisseurs de services comme La Poste donc de répondre aux attentes de ce nouvel écosystème en proposant des services utiles, innovants, socialement responsables et accessibles.

2) La Poste peut être le bras armé de l'Etat pour renforcer le climat de confiance et accélérer le développement de la transformation numérique de la société

L'un des enjeux principaux de la souveraineté numérique aux yeux de La Poste est celui de donner à nos clients - les entreprises, les administrations et les particuliers - la capacité de **maîtriser leurs données sur le plan technique, économique et juridique**. C'est non seulement souhaitable pour que l'émergence du numérique se fasse d'une manière sûre, respectueuse de nos principes et de notre souveraineté, mais c'est aussi nécessaire pour **accélérer la numérisation de l'économie française**. Nous constatons en effet qu'un certain nombre de nos clients freinent leur numérisation à cause de leurs craintes légitimes portant sur une exploitation de leurs données à caractère personnel ou commercialement sensibles, etc.

Dès lors, la confiance est selon nous au cœur de la problématique de souveraineté numérique. Le recours aux services de confiance nous paraît dès lors indispensable pour répondre aux principaux besoins de la vie quotidienne numérique, en toute sécurité :

a) Identification / authentification

Chaque jour, il est demandé aux usagers de s'identifier en ligne avec un niveau de sécurité plus ou moins important en fonction de la démarche effectuée. Une politique française d'identification numérique est nécessaire pour s'assurer que **des acteurs de confiance gèrent les données d'identité des personnes**. Elle doit répondre aux attentes des citoyens en matière de simplicité des usages.

L'Identité Numérique de La Poste permet de proposer dès aujourd'hui **un service d'identification et d'authentification protecteur des données personnelles et sécurisant les transactions des citoyens français** (notre solution est la seule qualifiée de niveau substantiel par l'Anssi).

Le modèle économique de l'identité numérique de La Poste repose sur une **stratégie d'acquisition d'utilisateurs adossée aux usages publics** – justifiant sa gratuité – et une **monétisation auprès du secteur privé**.

Nous avons **trois principales attentes** pour être en mesure de déployer très largement l'Identité Numérique de La Poste :

- il nous paraît indispensable de **développer les usages publics de niveau substantiel de** l'identité numérique via FranceConnect+. Les espaces numériques des acteurs publics doivent inscrire à leur agenda l'intégration de FranceConnect+ pour lutter contre la fraude ;

- il convient de développer des **usages privés** ;
- nous souhaitons **nous appuyer sur le déploiement de la carte d'identité électronique (CNIe) en France pour simplifier le parcours de création de l'identité numérique pour les Français**. Nous avons lancé un partenariat stratégique avec IN Groupe, proposant une solution qui repose sur l'utilisation du code PIN de la CNIe et qui permet de créer simplement et rapidement son identité numérique de niveau substantiel. **L'accord des autorités françaises est nécessaire pour avoir accès au code PIN de la CNIe.** Si cette possibilité lui est accordée, nous nous engageons à mettre en place ce système avant la fin 2021 pour le présenter à l'ANSSI.

Enfin, il convient prendre en compte **l'émergence des prestataires de vérification d'identité à distance** (PVID). Notre filiale Docaposte a également pour ambition de renforcer son positionnement dans ce domaine en proposant une nouvelle solution «PVID ». Ce service permet de développer des parcours clients plus simples, plus rapides et sécurisés pour lutter contre la fraude à l'identité.

b) Les échanges et les transactions sécurisées

La transaction numérisée correspond au transport d'informations ou de documents de manière sécurisée et prouvée. Il s'agit notamment de prouver l'identité des parties prenantes de la transaction, de garantir l'intégrité du contenu de la transaction et d'assurer son horodatage.

La sécurité des échanges électroniques devrait être au centre des préoccupations. **Les débats concernant l'encadrement du marché de la lettre recommandée électronique (LRE) dans le cadre du projet de loi « Daddue 2 » sont déterminants** [*Projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine des transports, de l'environnement, de l'économie et des finances*]. Il nous paraît important que la France fasse le choix d'un haut niveau de sécurité s'agissant des échanges électroniques sensibles et permettent l'émergence d'usages de ce service. Nous militons pour que ce projet de loi crée les conditions permettant aux **usagers de recourir facilement à la LRE dans leurs échanges avec les administrations**.

De la même manière, de nombreux échanges aujourd'hui s'effectuent par courriers électroniques au moyen des boites e-mails des personnes. Ces e-mails sont aujourd'hui, la plupart du temps, administrés par des grands acteurs du numérique ce qui ne permet pas de garantir la sécurité ou la maîtrise des données par les usagers. Le recours à des services sécurisés de messagerie permettrait d'améliorer la souveraineté numérique.

c) L'archivage et le stockage sécurisé des échanges dématérialisés

La conservation des données est aujourd'hui un enjeu incontournable, souvent le symbole de la souveraineté numérique et la maîtrise des données via les problématiques autour de la localisation des données. Nous sommes également convaincus que cette dimension est indispensable, c'est pourquoi nous nous engageons dans le projet européen Gaia-X, avec l'ambition de construire un écosystème numérique européen capable de rivaliser avec les grands acteurs du numérique.

Selon nous, une façon de promouvoir la souveraineté numérique auprès des citoyens serait d'articuler les **démarches publiques et privées numérisées les plus importantes avec des solutions souveraines de conservation de données**. Par exemple, nous proposons un service de boite aux lettres numérique, adossé sur un coffre-fort numérique appelé « Digiposte ». Ce service gratuit et ouvert à tous répond à un besoin des usagers de conserver leurs données et documents personnels, issus de sources différentes, dans un même endroit avec la garantie du maintien de leur intégrité et leur maîtrise.

Pour permettre aux citoyens de maîtriser leurs données, nous pensons qu'il serait pertinent d'**attribuer aux citoyens un « trousseau numérique »** avec une identité numérique, une messagerie sécurisée, un coffre-fort numérique, leur permettant de gérer leur vie numérique quotidienne.

3) Focus : œuvrer pour un numérique éducatif inclusif et sécurisé

Dans certains domaines, les enjeux de souveraineté sont particulièrement sensibles, comme c'est le cas pour l'éducation. Pour améliorer la souveraineté dans ce secteur, notre filiale Docaposte va lancer une expérimentation en **proposant son service de cloud pour les enseignants, adossé à sa solution PRONOTE** sur un département test. Nous nous proposons de partager les résultats de cette expérimentation dès sa finalisation.

La crise sanitaire a permis de faire émerger de nouveaux besoins pour le service public numérique éducatif. Il est important de **réaliser un état des lieux de ces nouveaux besoins des établissements scolaires et toute la communauté éducative en services numériques inclusifs et sécurisés.** La Poste et ses filiales Docaposte et Index Education sont prêtes à y contribuer.

Contribution de la Confédération française de l'encadrement, confédération générale des cadres (CFE-CGC)

CONFÉDÉRATION FRANÇAISE DE L'ENCADREMENT - CGC
ÉCONOMIE, INDUSTRIE, NUMÉRIQUE, LOGEMENT

7.5.2021

Assurer une souveraineté numérique française et européenne

La vision de la CFE-CGC

Le Numérique : un nouvel espace à conquérir et à façonner

Le Numérique est bien plus qu'une discipline. **Il dessine un nouvel espace, au même titre que l'espace aérien ou maritime,** dans lequel chaque citoyen, chaque entreprise évolue, échange, voire crée de la richesse. Evoquer la question de la souveraineté numérique, **c'est adresser les sujets traditionnels d'organisation territoriale, tels que la sécurité, l'autosuffisance, la régulation, la fiscalité, etc....**

Certains pays (Etats Unis et Chine) l'ont bien compris, mettant en œuvre très tôt des stratégies leur permettant de conquérir et s'approprier ce nouvel espace, ce qui faisait dire en 2013 à la sénatrice Catherine Morin-Desailly qu'à défaut de modification majeure de sa stratégie industrielle et politique pour le numérique, l'Europe pourrait devenir une « colonie numérique » de deux autres continents »[1].

Et les conséquences de cette absence de stratégie de conquête de l'espace numérique, ont et auront les mêmes effets sur le plan économique et social que ceux observés sur les délocalisations. **Car garantir notre souveraineté numérique c'est aussi assurer la pérennité de notre développement économique pour les années futures.** Faute d'ancrage dans un espace numérique européen, notre économie sera au mieux, dépendante, au pire en voie d'extinction.

Cette souveraineté entraine nécessairement la possibilité d'**assumer des choix**, comme l'indiquait Thierry Breton, cet été, dans une tribune au journal les Echos : *"Il ne s'agit pas de céder à la tentation de l'isolement ou du repli sur soi, contraire à nos intérêts, à nos valeurs et notre culture. Il s'agit d'assumer des choix qui seront déterminants pour le futur de nos concitoyens en développant les technologies et les alternatives européennes sans lesquelles il n'existe ni autonomie ni souveraineté."*

Pour la CFE-CGC, ces choix sont importants car **ils contribuent à défendre nos intérêts tant nationaux qu'européens, permettant de protéger nos compétences, nos entreprises, des pans entiers de secteurs d'activité, et garder ainsi une maîtrise de ces activités,** sans tomber dans un protectionnisme stérile en économie ouverte. Ces choix permettent aussi **la construction alternative aux deux mondes numériques proposés actuellement,** à savoir le capitalisme de surveillance américain ou le crédit social chinois. La souveraineté numérique permettra la construction d'un monde numérique tel que nous le souhaitons, respectant les valeurs françaises et européennes.

[1] Rapport 2013 Les enjeux d'une gouvernance du numérique à l'échelle européenne

Un espace numérique qui change la donne économique et sociale

Le numérique bouleverse le processus même de création de valeur, confiant à la donnée un rôle déterminant. La captation de valeur par les GAFAM, et le transfert opéré au détriment d'acteurs traditionnels (comme l'a montré l'Etude CSA Bearing Point sur le secteur des média[2]) illustre les conséquences économiques qui attendent les secteurs n'ayant pas intégré l'avantage comparatif procuré par l'exploitation des données. Cet avantage des BigTech vient d'ailleurs d'être mis en lumière par l'autorité de la concurrence dans son avis récent sur les Fintech et les Banques, en particulier dans le domaine stratégique des paiements.

Le numérique remet peu à peu en cause l'équilibre économique reposant sur la redistribution aux travailleurs d'une partie des richesses créées afin de favoriser la consommation des produits qu'ils fabriquent. **Cette transformation oblige à repenser la redistribution du partage de la valeur**. Nos fondamentaux économiques sont ébranlés, telle la capacité des Etats à lever l'impôt ou encore le financement de notre modèle de protection sociale pour ne citer que ces exemples.

Le numérique accroit ce phénomène de polarisation des emplois, se manifestant par l'effacement des emplois intermédiaires, et cela devrait se poursuivre selon les projections de l'OIT[3] ou de l'OCDE[4].

Les forces et faiblesses du secteur numérique en France et en Europe

Au regard de ces transformations qui s'opèrent, il nous semble important d'identifier nos forces et nos faiblesses pour mieux construire des propositions nous permettant de répondre aux **triples enjeux** d'obtention de notre autonomie numérique, à savoir :

- **Posséder l'infrastructure** et les outils indispensables à l'occupation de l'espace numérique ;
- **Maitriser les données** (carburant du numérique et créateur de richesse) sur l'ensemble de leur cycle de vie ;
- **Assurer la sécurité** de l'ensemble du territoire numérique mis en place (infrastructure, outils et données).

Cette souveraineté numérique au sens de la maîtrise et de l'autonomie stratégique nous permettra d'être pleinement acteurs de nos choix technologiques, innovants et forces de proposition sur les secteurs structurants de demain dans le numérique : Intelligence artificielle, 5G et IOT, blockchain, informatique quantique...

Des atouts :

- Les compétences reconnues de nos ingénieurs français ;
- Des entreprises acteurs du numériques dotées d'une taille suffisante pour construire les infrastructures (OVH, Atos, Thalès, etc...) nécessaires ;
- Un patrimoine de données très riche (ex sur la santé) ;
- Des entreprises françaises à la pointe dans la proposition de certaines solutions numériques comme Dassault System qui a réalisé plus de 50% des essais

[2] Etude CSA 2018
[3] Rapport 2019 Travailler pour bâtir un monde meilleur
[4] Rapport OCDE 2019 sur les perspectives de l'emploi

cliniques du vaccin contre la COVID19 sur ses plateformes, via sa solution de jumeau numérique (démontrant le déplacement de cette activité du monde physique vers le territoire numérique).

- Un RGPD qui pose les bases d'une régulation de la donnée ;
- Une épargne et un écosystème financier solide permettant d'accompagner le développement de l'économie du numérique.

Des faiblesses :

- Un flou entre les acteurs sur le sens à donner à la notion de « souveraineté numérique ».
- L'absence de sensibilisation des décideurs publics aux forts enjeux économiques nationaux et collectifs d'une perte de souveraineté : les services de renseignements français qui choisissent Palantir, les données du Health Data Hub confiées à Microsoft, Bpifrance qui choisit Amazon Web Service pour gérer les Prêts Garantis par l'Etat, etc....
- Un manque de soutien efficace au développement sur notre territoire des secteurs d'activité du numérique (cf. note CFE-CGC sur l'évolution de l'emploi salarié en France dans les Télécom a perdu, en poids relatif, 25% en dix ans).
- Le manque de coordination entre les services de l'Etat pour la mise en œuvre d'une vraie stratégie diffusée de notre souveraineté numérique, qu'ils s'agissent des compétences (appel d'offre licence 5 G minorant les enjeux de compétences et d'emplois sur le territoire national, compétences existantes potentiellement gâchées avec la fermeture du site de Nokia) ou de secteurs sensibles (renseignements, santé).
- L'absence de vraies règles de concurrence qui permettent de nous battre à armes égales avec les USA (ex : aucune contrepartie dans l'accord de libre échange entre l'UE et les USA sur le stockage des données qui permet un stockage des données aux USA et non en Europe) ; des règles de concurrence qui ont montré leur limite quand des « gros » rachètent des « petits » pour étouffer toute concurrence et en toute légalité (avec l'aval des autorités européennes et nationales).
- Un manque de puissance financière au regard des moyens financiers apportés par l'Etat américain (en particulier la DARPA).
- Le retard pris par l'Europe sur les infrastructures : *92% des données européennes sont sous Cloud étranger*[5]

Les propositions de la CFE-CGC

1. ***Sensibiliser les décideurs aux enjeux***

- Sensibiliser et faire de la pédagogie autour des conséquences économiques et sociales (à chiffrer) d'une perte de notre souveraineté numérique, afin que la souveraineté numérique devienne l'affaire de tous ;
- Définir un sens commun de la notion de « souveraineté numérique ».
- Comprendre le rôle des données (non personnelles) dans l'économie, et le fonctionnement des algorithmes et leur effet sur le jeu concurrentiel.
- Favoriser l'émergence de compétences féminines, pour construire un territoire numérique représentatif de notre société, puisque le monde numérique est appelé à dessiner les évolutions profondes de nos prochaines décennies.

[5] European Digital Sovereignty.pdf (oliverwyman.com)

2. ***Elaborer un plan de conquête et pilotage par le commissariat au Plan***

Confier au Commissariat au Plan, l'établissement d'un plan de conquête de notre souveraineté numérique, éclairé par les rapports institutionnels et parlementaires à l'image du Plan Calcul qui avait pour objectif d'assurer l'autonomie du pays dans les techniques de l'information.

3. ***Positionner un Etat Stratège qui coordonne les actions propices au développement d'un territoire numérique (y compris en proposant une régulation adaptée en lien avec l'Europe).***

- **Organiser un écosystème** équilibré économiquement et socialement (chaîne de valeur, politique fiscale, politique sociale : les gros ne sont plus des startups à protéger. Ce sont les ETI qui doivent pouvoir se consolider) ; et **qui soit propice à une mutualisation des technologies.**
- **Protéger certaines activités** (qui restent à définir) des règles du marché concurrentiel en fixant des contreparties obligatoires, des restrictions dans les appels d'offre ;
- **Comprendre et réguler le fonctionnement des algorithmes** et leurs effets pour mieux appréhender leur impact sur le jeu concurrentiel ; Interdire certains comportements (ex : la vente des données personnelles) ; Imposer dans le cadre de la négociation collective au sein des plateformes une négociation sur le thème de la lisibilité et transparence des algorithmes ; Afin de **limiter les prédations économiques reposant sur l'utilisation d'algorithmes,** encadrer les plateformes numériques et entreprises utilisatrices d'algorithmes**,** en créant **une structure conjointe CNIL et Autorité de la concurrence**, pouvant auditer et sanctionner les algorithmes (en cas d'abus de position dominante).
- **S'approprier le Data Governance Act (DGA),** Règlement de Gouvernance des Données, qui est à l'Economie, ce que le RGPD est à la Vie Privée, **r**èglementant la disponibilité des données, leur utilisation, leur fiabilité et leur sécurité ; et mettre en œuvre une vraie **politique de "Données d'Intérêt général"** (cf. Rapport Bothorel) pour **placer la création de valeur au niveau de l'analyse et non plus au niveau de la détention de la donnée** (ex: un des prochains enjeux sera la détention de données extra-financières).
- **Mettre en œuvre une sorte d'European Cloud Act**, sur le modèle du Small Business Act américain, obligeant les entreprises publiques à stocker leurs données dans un Cloud européen non soumis au Cloud Act américain, garantissant la protection des données des concitoyens ;
- **Protéger les startups/licornes émergentes** en repensant les parcours incubateurs, fonds d'investissements français qui favorisent uniquement leur éclosion sur le marché américain (exemple Dataïku) pour les accompagner à tous les niveaux de développement de l'entreprise.
- **Faire un bilan de notre corpus de protection des entreprises numériques** dites stratégiques afin de proposer une stratégie unifiée et lisible :
    - Bilan du décret Montebourg et extension sur les assets stratégiques.
    - Bilan du dispositif GCAS, Groupe de Contact d'Action et de Soutien aux entreprises d'intérêt stratégique vital, pour les entreprises de 10 à 200 salariés, mis en place par le Hub France IA

4. ***Accompagner les conditions d'émancipation d'un environnement technologique en s'appuyant sur nos propres forces***

➢ ***Faire de l'exemplarité des décideurs publics nationaux l'étendard du choix politique assumé***

Permettre aux entités publiques d'être des exemples : tirer les leçons de Palantir, du PGE ou du Health Data hub, et afficher une volonté politique claire pour permettre d'autres alternatives le moment venu :

- Développer les pôles d'excellence sur l'IA, comme le TeraLab ;
- Encourager les initiatives comme celle de Thales pour remplacer Palantir ;
- Être partie prenante voire partie civile sur les données à caractère personnel concernant la santé (Health Data Hub…) ;
- Alerter sur les dérives comme celle de la BPI.

➢ ***Donner de la visibilité aux solutions technologiques alternatives aux GAFAM :***

- Donner de la visibilité aux solutions technologiques numériques développées par les entreprises françaises et/ou sur logiciels libres : ex : Dassault System avec la réalisation sur technologie des jumeaux numériques des essais cliniques sur les vaccins Covid, ou encore les logiciels libres pour le lancement de SpaceX.
- Préférer les partenariats entre acteurs locaux (OVH, OBS) et éditeurs étrangers (Microsoft) à l'instar du partenariat stratégique Orange et Microsoft afin de maitriser les technologies et la localisation de nos données.
- Promouvoir et encourager les alternatives intéressantes : ex Liibre ;
- Sensibiliser les grandes entreprises à leur dépendance aux outils Microsoft, Oracle, SAP…
- Réfléchir à des alternatives crédibles sur toute l'offre ou sur certains produits (concurrents à Office, Yammer, Teams…) ;
- S'inscrire dans la stratégie européenne de l'open source et aider dans cette perspective l'écosystème open source français (CNLL, l'Union des Entreprises du Logiciel Libre et du Numérique Ouvert, membre de l'APELL, l'Association Professionnelle Européenne du Logiciel Libre).

5. ***Drainer l'épargne des particuliers vers un fonds d'épargne grand public orienté sur la souveraineté numérique. Nouveau Capitalisme français.***

Un tel fonds permettrait de financer les entreprises françaises et européennes contribuant à assurer notre souveraineté, apporter une force de frappe supplémentaire au parcours de l'accompagnement des entreprises dans le capital risque, pour le passage à l'échelle (cf note CFE-CGC sur le sujet).

6. ***Mobiliser autour des compétences pour être du bon côté de la polarisation***

➢ **Elaborer une GPEC Numérique** (Gestion Prévisionnelle des Compétences Numériques) en identifiant les compétences numériques clés répondant à la trajectoire nationale fixée pour asseoir notre souveraineté numérique.
➢ **Protéger les compétences pour aujourd'hui** (Nokia sur la 5G ou la cybersécurité) **ou pour demain** en limitant ou contrôlant (cahier des charges pédagogiques) les partenariats public-privé (écoles IA Microsoft / Simplon, Facebook, IBM écoles) ;

- **Faire la consolidation des résultats des EDEC** sur le numérique menés dans les différents secteurs pour avoir la vision la plus globale possible sur les besoins et défis en termes d'emplois et de compétences.
- **Assurer la mixité des parcours d'enseignement supérieur** débouchant sur des métiers du numérique, en donnant envie à des jeunes filles d'embrasser des carrières numériques (cf. initiative Numeriqu'elles), voir en imposant dans des cursus un niveau minimal pour le sexe le moins représenté, et garantir la mixité.
- **Répondre à la transformation des compétences par l'adaptation des métiers à la « compétence donnée »** via des formations ajustées par niveaux (socle de « culture data », hybridation métier, métier de la donnée).
- **Assurer une obligation de formation sur la cybersécurité de tous les salariés appelés à utiliser des outils numériques** : on dit que 90% des cyberattaques proviennent d'une « erreur » produite entre le clavier et la chaise.

7. *Faire un focus spécifique sur la cybersécurité*

Compléter notre corpus en cybersécurité (Indépendance des RSSI à l'instar des DPO, audit de la sécurité des systèmes d'information par organismes indépendants, cartographie des interconnexions des réseaux des grandes entreprises ou OIV (Exemple : Orange CyberDéfense, Dataiku).

8. *Articuler la vision nationale et la vision européenne au niveau européen*

- Partager la vision nationale au niveau européen :
  - Pousser cette vision au niveau européen et promouvoir des partenariats entre pays européens pour mutualiser les maturités, les savoirs et les savoir-faire :
    - Inviter les acteurs français à être plus présents dans les grands dossiers de régulations européennes (IA, 5G, IOT) ;
    - Promouvoir l'interopérabilité des solutions françaises pour s'inscrire dans les standards européens (ex : Stopcovid).
  - Consolider l'influence normative de la France sur la politique européenne de la donnée avec la création de la notion de donnée à forte valeur ajoutée, directement inspirée de la donnée de référence, issue de la loi française pour une république numérique de 2016, avec la forte ouverture proposée par le rapport Bothorel pour les données du secteur public, mais aussi privé.

- Partager la vision européenne au niveau national, notamment sur le Cadre sécurisé de la 5G via la déclinaison de la 5G tool box européenne :

  A ce titre, la boite à outils identifie un ensemble de mesures à la fois stratégiques et techniques sur lesquelles pourront s'appuyer les Etats membres afin de faciliter la **mise en œuvre des réponses nationales**.

Les actions de la CFE-CGC sur le thème de la souveraineté numérique

EDEC (Engagement Développement Et Compétences) sur l'IA aux côtés du MEDEF et d'OPCALIA : https://travail-emploi.gouv.fr/emploi/accompagnement-des-mutations-economiques/appui-aux-mutations-economiques/edec
Membre du comité de pilotage de l'EDEC Perspective IA dont l'objectif est d'accompagner les entreprises et leurs salariés aux enjeux de l'IA (connaissance, usages et opportunités).
Implication dans les évènements de LaREFNum comme lors de la table ronde sur les compétences et transformations économiques : les impacts de l'IA, du 10 novembre 2020 : #LaREFnum20 | Compétences et transformations économiques : les impacts de l'IA

Projet SeCoIA Deal : « Servir la Confiance dans l'Intelligence Artificielle par le dialogue » https://twitter.com/SecoIADeal
Projet (2021-2023) piloté par la CFE-CGC avec un soutien financier européen réunissant des acteurs de divers horizons (syndicats français, italiens suédois, européens, des représentants d'entreprise de proximité, des acteurs institutionnels internationaux et des acteurs de la société civile (ONG et fondation) ;
Objectifs : Comprendre le futur du travail à l'ère de l'IA pour mieux construire le dialogue social de demain. Eclairer et définir le partage de la valeur créée à partir de la donnée (gain de productivité) pour mieux accompagner cette transformation des compétences et des emplois.
Chaire "Gouverner l'organisation numérique"
Membre de cette chaire lancée en mars 2021 dont l'objectif est d'étudier l'impact de la production et de l'exploitation des données numériques sur les organisations en vue de mieux gouverner ce nouvel espace.

Suivi de mise en place du GAIA-X dans le hub France piloté par le CIGREF
GAIA-X est un projet de services de Cloud européen. L'ensemble des fournisseurs de cloud européens (ou non) pourront proposer leurs services à travers l'offre GAIA-X s'ils respectent le cahier des charges exigeant mis en place par l'association GAIA-X.

Il y un risque que les gros fournisseurs comme Amazon, Google ou Alibaba essaient de modifier ces contraintes pour les rendre moins contraignantes, ce qui serait un échec en termes de souveraineté. C'est à ce titre que nous souhaitons nous investir au niveau français et européen afin de vérifier que les objectifs initiaux du projet GAIA-X soient bien respectés.

Contribution du Mouvement des entreprises de taille intermédiaire (METI)

Paris, le 20 janvier 2021

Mission d'information de l'Assemblée Nationale
« Bâtir et promouvoir une souveraineté numérique nationale et européenne »

CONTRIBUTION DU MOUVEMENT DES ENTREPRISES DE TAILLE INTERMEDIAIRE (METI)

La transformation numérique des entreprises de taille intermédiaire (ETI) se joue aujourd'hui dans un contexte de fragilisation du tissu économique. Reconnues pour leur résilience en temps de crise, elles sont aujourd'hui très affaiblies par les trois trimestres de crise que nous venons de traverser : leur capacité d'investissement s'est dégradée et elles sont désormais exposées à un risque de prédation (I).

Malgré leurs difficultés, **les ETI ont accéléré leur transformation numérique en 2020.** C'est le sens des principaux enseignements du baromètre 2020 de la maturité digitale des ETI réalisé en décembre 2020 en partenariat avec EY, Apax Partners et avec le soutien de l'institut CSA (II).

Pour continuer à se transformer, elles doivent désormais concilier les enjeux de court terme (adaptation au contexte de crise) à des enjeux de long termes (projets complexes et coûteux à même de conférer un avantage compétitif, notamment par rapport à la concurrence étrangère).

La transformation numérique des ETI étant étroitement liée à leur capacité d'investissement, la restauration de la compétitivité du « site France » sera un élément essentiel pour permettre à ces entreprises de mener à bien leur transformation numérique.

Enfin, pour pouvoir opérer une transformation digitale qui réponde aux enjeux de souveraineté numérique, en particulier concernant l'utilisation des données, les ETI auront besoin d'être **davantage accompagnées et soutenues par la puissance publique**, notamment via la commande publique.

I. La transformation numérique des ETI se joue aujourd'hui dans un contexte de fragilisation du tissu économique

Rappel des chiffres clés :

- 5400 ETI en France (8000 en Italie, 10 500 au Royaume-Uni et 12 000 en Allemagne)
- 68% des sièges sociaux situés hors de l'Ile-de-France, 75% des sites de production situées en régions
- 25% de l'emploi ; 38% des emplois de l'industrie manufacturière
- 335.000 emplois nets créés entre 2009 et 2015
- 34% des exportations pour 4% des exportateurs ; 3/4 des ETI présentes à l'international

Impact de la crise COVID-19 :

- Évolution moyenne du CA estimée pour les ETI pour l'année 2020 (vs. 2019) : -6,1 %
- Évolution moyenne du CA à l'export constatée en 2020 (par rapport à 2019) : - 6,9 %
- Plus d'1 ETI sur 2 a connu une baisse de son chiffre d'affaires en raison du deuxième confinement.
- Près de la moitié des ETI font état d'un niveau de leur carnet de commande en baisse ou en forte baisse par rapport à l'an dernier
- Un peu plus de la moitié des ETI ont vu leur capacité d'investissement se dégrader avec la crise, il en va de même pour le ratio endettement/fonds propres
- Plus de 4 ETI sur 10 ont connu une diminution de leurs effectifs depuis janvier 2020

- En 2020, une ETI sur 10 a récemment fait l'objet de tentative(s) étrangère(s) d'entrée au capital ; la proportion est équivalente s'agissant des tentatives étrangères de rachat.

II. Malgré la crise économique, la transformation numérique des entreprises de taille intermédiaire accélère : la maturité digitale des ETI a progressé en 2020

- **Principaux enseignements du baromètre 2020 de la maturité digitale des ETI réalisé par le Meti en partenariat avec EY et Apax Partners et avec le soutien de l'institut CSA – déc. 2020**

A. <u>La maturité digitale des ETI progresse en 2020</u>

- Plus de 2 ETI sur 3 sont activement engagées dans leur transformation digitale

B. <u>La crise sanitaire a accéléré la transformation digitale des ETI et transforme progressivement l'organisation de travail dans les entreprises</u>

- Les ETI se sont distinguées dans la crise par leur capacité d'adaptation : 84% des ETI étaient prêtes à affronter la crise
- La crise a accéléré le recours aux outils digitaux pour 92% des ETI : messagerie instantanée, visioconférence, outils de transfert de fichier, renforcement de l'e-commerce

C. <u>Les ETI investissent toujours plus massivement dans le digital</u>

- 71% des ETI déclarent vouloir accélérer leurs investissements dans le digital
- 1 ETI sur 2 déclare que la crise a accéléré le déploiement d'outils d'amélioration de l'expérience client et de transition vers le marketing digital
- Les ETI priorisent leurs investissements de manière pragmatique avec un retour sur investissement rapide : outils digitaux et collaboratifs, amélioration de l'expérience client, modernisation des infrastructures IT, cyber sécurité

D. <u>La direction générale joue un rôle déterminant pour créer et maintenir la dynamique</u>

- 71% des ETI déclarent la direction générale et la DSI comme porteuses principales de la transformation digitale de leur entreprise
- La transformation digitale se heurte à quelques freins bien identifiés : résistance au changement, manque de vision partagée et difficultés à intégrer de nouvelles compétences

III. Les ETI ont besoin d'être accompagnées et soutenues par la puissance publique pour opérer une transformation digitale qui réponde aux enjeux de souveraineté numérique

Les enjeux de souveraineté numériques se caractérisent essentiellement, au niveau des ETI, par un manque de lisibilité et de stabilité : difficultés à identifier des opérateurs français ou européens pour récolter, sécuriser et analyser leurs données (offres Paas, Saas, cybersécurité, Cloud) ; incertitude juridique autour du transfert et de la localisation des données (cf. invalidation du *Privacy Schield* par la Cour de Justice de l'Union Européenne, 16 juillet 2020).

En outre, les enjeux de souveraineté numérique sont aujourd'hui exacerbés par l'impact de la crise COVID-19 (risques accrus en termes de cybersécurité[1], prédations étrangères, endettement) et nécessitent des **mesures structurelles,** à la fois **d'accompagnement** (acculturation, orientation, certification) **et de soutien des ETI**, via la commande publique, en particulier en matière de données et de cloud, où il y a urgence à agir.

➢ **Propositions pour contribuer à restaurer la compétitivité du « site France » et assurer la souveraineté du tissu d'ETI sur le long terme**

1. **Assurer le déploiement rapide et efficace du plan de relance au niveau des ETI,** notamment sur son volet numérique, et bien veiller à ce que ce dernier soit adapté à leurs besoins (cf. volumes de subvention limités par les régimes d'aides d'État).

2. **Confirmer, si ce n'est amplifier la trajectoire de baisse de fiscalité de production engagée par le gouvernement,** qui constitue le premier levier de transformation des ETI en restaurant leurs capacités d'investissement de façon durable et tangible.

   N.B. La baisse de la fiscalité de production est la mesure du plan « France Relance » répondant le plus aux besoins des ETI (63,3%), devant les aides à la digitalisation et à la robotisation (20%).
   Source : enquête METI n°17 réalisée auprès de 800 ETI, novembre 2020.

3. **Mettre en place un « Pacte très long terme » pour faciliter la transmission d'entreprises face aux risques avérés de prédation en alignant le coût de la transmission sur la moyenne européenne tout en protégeant les noyaux durs d'actionnaires de long terme.** Celui-ci prévoirait un abattement des droits à hauteur de 90%, en contrepartie d'une obligation de conservation des titres portée à 10 ans.

➢ **II. Propositions pour accompagner la transformation numérique des ETI**

4. **Pérenniser, voire renforcer les dispositifs de soutien qui ont fait leurs preuves** (ex : CIR) et promouvoir tout AAP/toute subvention auxquels sont éligibles les ETI

5. **Élargir l'initiative France Num pilotée par la DGE aux ETI** qui sont pour le moment exclues de ce dispositif d'accompagnement

[1] "76% des dirigeants d'ETI ont subi au moins une incidence cyber en 2019 et la montée du risque s'accélère avec des conséquences importantes (défaillances, pertes de valorisation, réputation)" (source : *Étude Bessé, 2021).*

➢ **III. Propositions pour renforcer la souveraineté numérique française et européenne, en particulier concernant l'utilisation des données :**

6. **Promouvoir la qualification SecNumCloud de l'ANSSI** pour aider les entreprises et les collectivités territoriales à identifier des offres de cloud de confiance qui garantissent la protection et la souveraineté des données

7. **Établir un label « de confiance »,** moins contraignant que le SecNumCloud, qui permettrait d'identifier rapidement les services remplissant la condition de souveraineté numérique, voire de non-utilisation de la donnée des clients, pour les solutions digitales nécessitant un niveau de sécurité d'utilisation inférieur.

8. **Soutenir la souveraineté numérique, technologique et industrielle française via la commande publique** à l'aide notamment d'une reconnaissance plus forte du « Made in France » ou du « Made in Europe » dans les appels à projets ; d'un appui renforcé de l'administration pour le développement des solutions souveraines et l'expérimentation autour du C2 (cercle de solutions destinés à traiter les données sensibles).

9. Renforcer l'accompagnement des ETI en matière de cybersécurité, par exemple par le biais de l'ANSSI

Contribution du Mouvement des entreprises de France (MEDEF)

MEDEF

Contribution écrite

Suite audition L. Giovachini et Ch. Poyau du 14/01/2021

Mission d'information Assemblée Nationale

Bâtir et promouvoir une souveraineté numérique nationale et européenne

LE MEDEF EN QUELQUES CHIFFRES CLES

- 173 000 entreprises adhérentes au travers de 91 fédérations professionnelles regroupant l'ensemble des secteurs d'activité (industrie, service, construction, commerce…),
- 14 organisations associées et partenaires, et
- 122 organisations territoriales en France métropolitaine et en outremer.
- 95% des entreprises adhérente au MEDEF sont des TPE/PME/ETI, pour une taille moyenne de 47 salariés.

- Qu'il s'agisse de protection des données des entreprises, de régulation des acteurs du marché, de développement et de facilitation de recours à des outils sécurisés, ou de technologies d'avenir, nous défendons au MEDEF une approche offensive de renforcement de notre souveraineté numérique qui couvre à la fois les questions régaliennes, l'intérêt économique et des sujets sociétaux.

- Les enjeux aujourd'hui :
  - Être en capacité de maitriser son destin
  - Réduire ses dépendances pour être plus autonome, mais sans verser dans l'autarcie.
  - Renforcer ses capacités à affronter des crises et à rebondir et donc devenir plus résilient.
  - Se donner également les moyens d'être compétitifs sur les marchés internationaux face à nos concurrents étrangers, de devenir leader sur des technologies d'avenir et garder un esprit de conquête.
    Défendre et renforcer nos positions dans la compétition mondiale, c'est assurer l'avenir de l'Europe.

Articuler le tryptique *« protéger, ne pas entraver et rester attractifs »*.

- Les entreprises ne veulent pas se trouver « disruptées » ou dépendantes de solutions concentrées sur un tout petit nombre d'acteurs. La souveraineté peut en effet venir, soit de la maîtrise de la technologie, soit de la diversité des sources… afin de ne pas dépendre d'un seul fournisseur venant d'une seule zone géopolitique.

- La souveraineté numérique, c'est aussi récupérer la maîtrise de ses données (que ce soit pour les citoyens ou les entreprises) et assurer une plus grande protection des données stratégiques des entreprises, ce qui nécessite de renforcer la cybersécurité en Europe et de promouvoir une sécurité efficace à moindre coût.

- Une meilleure maîtrise des données ne passe pas forcément par une localisation forcée des données (personnelles ou non-personnelles), mais par une plus grande transparence, et la possibilité de choisir un partenaire ou prestataire de confiance.

- Nous recommandons l'adoption d'une approche pragmatique de cercles géographiques concentriques, permettant de définir plus clairement :
    - Ce qui doit impérativement être maîtrisé sur le territoire national, car enjeux sensibles et critiques ;
    - Ce qui relève du niveau européen et peut être soutenu par les différentes politiques et initiatives européennes, comme par exemple GAIA-X, auquel le MEDEF a adhéré ;
    - Ce qui peut être fait en partenariat avec des acteurs internationaux pour répondre aux besoins de développement de nos entreprises sur la scène mondiale.

- Cette approche ne pourra se matérialiser de manière efficace et pertinente que si elle repose sur des partenariats public-privé plus étroits.

- Si les enjeux numériques sont intégrés dans le plan FranceRelance, celui-ci nous semble toutefois appréhender de manière insuffisante les problématiques de transformation numérique liées à la révolution des plateformes et de la donnée.

- Il nous faut impérativement entrer dans une économie de la donnée.
    - Derrière les géants du numérique, c'est une nouvelle typologie d'entreprise et une nouvelle façon d'offrir des services : une plateforme avec des marchés « bi-face » où le client apparent n'est pas celui qu'on croit.
    - Les plateformes créent des effets de réseau dans lesquels la valeur n'est plus seulement dans le produit ou le service délivré mais dans le fait que des milliers voire des millions de personnes passent par la plateforme pour accéder à un produit ou à un service.

  Derrière cet effet de réseau, la prise de conscience par les entreprises du potentiel des données dont elles disposent pour valoriser leurs activités, et comme source d'innovation et de croissance est cruciale.

- Il y a une nécessité absolue que les entreprises françaises de tous secteurs participent plus à la construction de la règlementation qui pourraient avoir tendance à se faire avec les plus gros acteurs

MEDEF

REPONSE AU QUESTIONNAIRE

Proposer un bilan de l'impact de la crise épidémique de la Covid-19 sur les entreprises que vous représentez. Comment ces entreprises envisagent-elles les prochains mois ?

- Du côté entreprises, tous les secteurs n'ont pas été impactés de la même façon : globalement l'économie tourne à 90% de la normale et l'année 2020 devrait se solder par une contraction du PIB de l'ordre de 9%. Certains secteurs ont subi une perte d'activité de l'ordre de 30% sur l'année 2020, à l'image de l'hébergement-restauration, la cokéfaction et raffinage, et la fabrication de matériel de transports.

- Aussi paradoxal que cela puisse paraître, les défaillances d'entreprises ont reculé de 35% sur un an : cela s'explique par l'ensemble des dispositifs mis en place par la puissance publique qui ont permis aux entreprises de tenir le coup. Cependant, le ciblage imparfait des aides a permis d'éviter les défaillances d'entreprises performantes au prix du maintien d'entreprises peu performantes et/ou non viables (zombification de l'économie).

- Se pose le problème de la dette des entreprises : celle-ci était déjà importante avant la crise de la Covid et s'inscrivait sur une dynamique haussière depuis une dizaine d'année (contrairement à ce que l'on pouvait observer pour les entreprises allemandes, espagnoles et italiennes). Or l'excès d'endettement détruit de la valeur (soit par le biais de faibles incitations à investir, soit par celui de liquidations excessives) ce qui constitue un risque pour notre croissance potentielle... déjà bien faible.

- Ce qui est clair est qu'une majorité d'entreprises, particulièrement au sein des TPE-PME, ont dû, dans l'urgence, accélérer leur digitalisation. Et force de constater qu'elles ont principalement eu recours aux solutions des GAFAM (ex : Zoom, Teams).

- Globalement, les perspectives des entreprises ne sont pas au beau fixe (avec néanmoins des différences en fonction des secteurs ; les secteurs de l'économie présentielle – hébergement-restauration, événementiel, culture, sport – sont particulièrement inquiets sur leur avenir, ne disposant pas de calendrier de réouverture) en raison de l'incertitude sanitaire et d'une demande affaiblie ; le retour de la confiance est notamment conditionné à l'évolution sanitaire (vaccin) et à la visibilité qui sera apportée sur la façon dont le sujet de la dette sera traité.

Comment concevez-vous la notion de souveraineté numérique française et européenne ? De quelle façon cet impératif peut-il se traduire concrètement pour les entreprises que vous représentez ?

- La souveraineté est le pouvoir suprême reconnu à l'État, qui implique **l'exclusivité de sa compétence** sur le territoire national *(souveraineté interne)* et son **indépendance absolue** dans l'ordre international où il n'est limité que par ses propres engagements *(souveraineté externe).*

MEDEF

- Il est possible de parler de la **souveraineté à l'ère numérique** : **le numérique** mettant en question les monopoles régaliens, soit parce qu'il **crée des acteurs de substitution**, soit parce qu'il **fragilise les outils régaliens**. Ainsi des **acteurs rivalisent avec des Etats** dans la mise en place de capacité régalienne (crypto monnaie comme LIBRA, l'identité numérique, violence légitime (ex le « hack back ») ...

- Si l'on se focalise plus particulièrement sur la souveraineté numérique, qui couvre la protection de l'innovation, des compétences et des savoirs français et européens (propriété industrielle, secrets d'affaires, compétences...), **plusieurs aspects se mélangent : les questions régaliennes, l'intérêt économique et des sujets sociétaux, tous ayant été particulièrement éclairés par la crise COVID.**

- La souveraineté numérique est devenue une part importante de la souveraineté économique en ce **que les entreprises ne veulent pas se trouver « disruptées » ou dépendantes de solutions concentrées sur un tout petit nombre d'acteurs**. La souveraineté peut en effet venir soit de la maîtrise de la technologie soit de la diversité des sources... afin de ne pas dépendre d'un seul fournisseur venant d'une seule zone géopolitique.

- **La question de savoir si la France / Europe a perdu ou serait en train de perdre sa souveraineté à l'ère numérique et / ou dans l'espace numérique** s'est imposée à nous avec d'autant plus d'acuité que **les questions de lutte commerciale internationale se sont accrues avec force sous l'administration Trump, le déploiement de la 5G et des équipementiers autorisés ou non, de l'accroissement fulgurant des usages numériques pendant les confinements.**

- Et les entreprises ne sont pas les seules à avoir cette prise de conscience**. L'Etat français, en réformant son dispositif de défense économique avec un rôle clé confié au SISSE (ainsi qu'à l'ANSSI), est particulièrement moteur à l'échelle européenne sur les sujets de souveraineté économique et numérique.** Les travaux animés par le SISSE sur le Cloud Act, l'executive order pris par Donald Trump en mai 2019 contre Huawei en sont l'illustration.

- Le SISSE n'a pas d'équivalent en Europe et nous constatons au niveau de nos propres homologues européens les difficultés de mobilisation pour construire à l'échelle européenne un arsenal réglementaire adapté pour nos entreprises.

- **La souveraineté numérique, c'est aussi récupérer la maîtrise de ses données** (que ce soit pour les citoyens ou les entreprises) **et assurer une plus grande protection des données stratégiques des entreprises,** ce qui nécessite de **renforcer la cybersécurité en Europe et de promouvoir une sécurité efficace à moindre coût**.

- **Une meilleure maîtrise des données ne passe pas forcément par une localisation forcée des données (personnelles ou non-personnelles), mais par une plus grande transparence** (par exemple : information en cas de demande d'accès à des données d'entreprises par des autorités françaises ou étrangères lorsque ces données sont hébergées chez un tiers) **et la possibilité de choisir un partenaire ou prestataire de confiance.**

- **Il ne faut pas que la souveraineté numérique se traduise concrètement par des exigences de localisation systématique des données en France ou en Europe.**

1. **Protection des données stratégiques**

Il ne faut pas confondre la localisation des données et la volonté de protéger les données stratégiques des entreprises en utilisant des infrastructures ou des solutions sécurisées qui ne sont pas soumises à des lois étrangères.

En effet, le CLOUD Act permet l'accès par les autorités américaines à des données détenues par des fournisseurs de services américains ou en lien avec les Etats-Unis (« *US Person* »), quel que soit le lieu où les données sont détenues. **La localisation physique des données n'est donc pas un critère permettant d'échapper à l'extraterritorialité des lois de renseignement américaines.**

C'est en ce sens qu'il faut :

- **Développer des solutions et infrastructures de confiance** (plutôt que « souveraines ») qui permettent de sécuriser les données et de protéger les entreprises en cas d'accès par des autorités (qu'elles soient françaises, européennes ou étrangères) en les informant de cette demande d'accès (et des données concernées). Du point de vue des entreprises, la problématique est la même pour les textes européens (e-evidence) et américains (CLOUD Act).
- Promouvoir les politiques d'ouverture des données publiques tout **en s'assurant que ces politiques ne mettent pas en risques les acteurs économiques sensibles (OIV, OSE) et le savoir (propriété intellectuelle, savoir-faire) français.**
- **Ne pas imposer le partage de données des entreprises et les conditions de partage,** mais encourager le partage volontaire dans le cadre de partenariats économiques.

2. **Les échanges de données au niveau international sont aujourd'hui fondamentaux, pour le commerce électronique, mais plus généralement pour le développement international des entreprises françaises.**

Outre l'utilisation de solutions informatiques, les flux de données sont en effet incontournables quand une entreprise s'installe à l'étranger (données RH des salariés expatriés, données pour assurer la sécurité des salariés à l'étranger…), quand elle développe son activité à l'étranger (données des clients étrangers, échanges de données au sein d'un groupe…) ou quand elle négocie des contrats avec des fournisseurs, clients ou partenaires étrangers.

L'interprétation par le Comité européen de protection des données (CEPD) et la CNIL de la décision de la CJUE (16 juillet 2020) dite « Schrems II » est très stricte et empêche in fine les transferts de données personnelles hors UE et par conséquent le développement international des entreprises européennes.

MEDEF

L'équilibre à trouver est d'assurer la protection des données (des individus et des entreprises) européennes, tout en tenant compte des réalités et besoins économiques.

Imposer la localisation des données et l'utilisation de solutions souveraines entraverait la liberté d'entreprendre et la liberté de choix des cocontractants pour les entreprises, sans toutefois régler la question des compétences extraterritoriales de certaines autorités étrangères.

Outre les initiatives privées, il conviendrait davantage d'encourager la conclusion d'accords politiques entre l'UE et les US sur les données (Privacy Shield, CLOUD Act…) **afin d'instaurer des procédures claires quant à l'accès aux données et poser comme principe la transparence vis-à-vis des demandes d'accès à des données détenues par des entreprises.**

Focus sur les initiatives telles que OVH/Google : si ces solutions semblent offrir des garanties techniques, certaines entreprises sont mitigées, car elles considèrent que, du fait de Google, ces initiatives restent soumises légalement au droit américain et donc au CLOUD Act.

- **De quelle façon les pouvoirs publics peuvent-ils promouvoir une forme de souveraineté numérique française et européenne, selon vous ?**

Il semble difficile pour un Etat « stratège » de ne pas se tromper dans les choix de technologies à soutenir, c'est pourquoi il nous semble important de travailler à des outils et actions de diverses natures : de financement, garanties d'Etats, amélioration des marchés publics innovants… avec des effets de leviers ; avec une gouvernance multipartite attentive semble également impérative.

Les « politiques publiques »

- **Soutien financier** : Par un cadre adapté aux start-ups, au soutien à la recherche ou l'accès à la commande publique.

- **Soutien administratif, règlementaire et politique** pour que les entreprises puissent bénéficier d'un cadre et d'outils préservant leurs capacités à décider et agir en toute autonomie :

    - par une lutte renforcée contre les **ingérences et initiatives de déstabilisation économiques étrangères** (ex : prises de contrôles et investissements étrangers, extra-territorialité du droit, espionnage économique et industriel, fonds activistes…) ;
    - par la protection de la **de sécurité numérique** : lutte contre les différents types de cyberattaques et de déstabilisation par les flux d'information; le développement d'une culture de sécurité économique au sein des entreprises.
    - **Par une pédagogie accrue sur les usages numériques**, le recours à des solutions sécurisées et de confiance (ex : messageries, visioconférences, solutions cloud…) la lutte contre la fracture numérique et en montrant également l'exemple sur ces sujets.

MEDEF

- **La commande publique vous semble-t-elle suffisamment accessible pour les entreprises et orientée vers des solutions technologiques souveraines ? Si non, avez-vous des propositions à formuler sur ce sujet ou des exemples de dispositifs étrangers dont il serait possible de s'inspirer ?**

La commande publique n'a pas été conçue pour prendre en compte les enjeux de souveraineté et les solutions technologiques souveraines.

Au-delà de la commande publique, la mise en place de partenariats public/ privé nous semble devoir être renforcée, en ce que ce type de collaborations permet d'anticiper très en amont les grands changements technologiques en les accompagnant dès le départ par un soutien de l'Etat et en construisant les débouchés en même temps que les solutions sont élaborées.

- **Comment jugez-vous le soutien de la puissance publique à la numérisation des entreprises ? Que pensez-vous, dans ce cadre, du plan « France Relance » qui contient des mesures destinées à la promouvoir *via* France Num ?**

Le MEDEF œuvre à une prise de conscience par les entreprises de l'impérieuse nécessité de se numériser et de valoriser les entreprises françaises et européennes qui agissent en ce sens.

La crise sanitaire a eu cet effet positif d'une accélération majeure des usages qui arrive dans un contexte où la fibre est déployée à « marche forcée » et donc permet aux entreprises de se « connecter » à un haut / très haut débit de plus en plus facilement.

La **crise du Covid a accéléré les usages**, par exemple dans de nombreux domaines : en télémédecine ; télétravail ; l'achat en « click & collect » ; le développement en général d'une économie sans contact (paiement sans contact utilisation de QR Code, couramment utilisé en Asie avant la crise, son usage s'est également largement développé en Europe).

Si les enjeux numériques sont intégrés dans le plan de relance, celui-ci nous semble toutefois appréhender de manière insuffisante les problématiques de transformation numérique liées à la révolution des plateformes et de la donnée.

La numérisation des entreprises est souvent un processus difficile, car le numérique, ce n'est pas seulement installer un logiciel ou acquérir quelques PC : c'est potentiellement changer de business model. En cela, **le plan de relance nous semble une opportunité à ne pas manquer. Or aujourd'hui il nous semble que tant dans les montants que dans les modalités nous n'y sommes pas.**
Par exemple *la subvention « Industrie du Futur » (numérisation des ETI et PME industrielle) introduite par le plan de relance viendrait d'être « rabotée » ; lancé en octobre elle serait « victime de son succès » et le gouvernement réduirait en conséquence le taux de soutien pour les nouvelles demandes de subvention, qui passerait de 40% à désormais 10% ! (cf. intervention A. Pannier-Runacher).*

Ce changement de dernière minute du dispositif est très problématique pour les entreprises qui avaient prévu de demander la subvention avec un taux de 40% pour 2021.

MEDEF

En effet, **il nous faut impérativement entrer dans une économie de la donnée.**

- Derrière les géants du numérique, c'est une **nouvelle typologie d'entreprise et une nouvelle façon d'offrir des services** : une plateforme avec des marchés « bi-face » où le client apparent n'est pas celui qu'on croit.
- Les plateformes créent des **effets de réseau** dans lesquels la valeur n'est plus seulement dans le produit ou le service délivré mais dans le fait que des milliers voire des millions de personnes passent par la plateforme pour accéder à un produit ou à un service.

Derrière cet effet de réseau, la prise de conscience par les entreprises du potentiel des données dont elles disposent pour valoriser leurs activités est cruciale.

- **Que pensez-vous, également, des mesures de relance destinées à garantir une forme de souveraineté technologique française ? Quels sont, selon vous, les secteurs technologiques qui nécessiteraient une vigilance accrue des pouvoirs publics vis-à-vis de leur caractère critique ? Pour quelle(s) raison(s) ?**

  - Le Medef se félicite de l'intégration d'un volet expressément dédié à la souveraineté technologique au sein du plan de relance (ex : appels à projets dans 5 secteurs stratégiques et mesures du PIA 4 qui porte sur de nombreuses technologies d'avenir).

  - L'enjeu est une mise en œuvre effective de ces mesures, que Bercy vient juste de détailler le 8 janvier dernier.

  - Pas de commentaires à ce stade sur les secteurs technologiques nécessitant une vigilance particulière.

- **La cybersécurité est une composante à part entière de la souveraineté. Comment les entreprises françaises, que vous représentez, appréhendent-elles la gestion de ce risque ? Ont-elles des besoins, demandes spécifiques à formuler sur ce sujet ?**

  - La cybersécurité est le pendant de la transformation numérique et il est absolument fondamental de sensibiliser les acteurs à ces enjeux.

  - Toutefois, **il faut tenir compte des réalités économiques** : les entreprises n'ont pas toutes les moyens (financiers, techniques ou humains) d'assurer le même niveau de sécurité que des opérateurs d'importance vitale (OIV) ou de services essentiels (OSE).

  - **Il est nécessaire de développer des solutions de sécurité informatique qui soient efficaces et accessibles à l'ensemble du tissu économique, y compris les TPE/PME.**

MEDEF

La présente mission d'information travaille également sur les enjeux de concurrence et de fiscalité du numérique. Quelle est votre position sur ces sujets ?

- Concernant la concurrence, le **MEDEF soutient les initiatives européennes sur les services et marchés numériques (DSA/DMA)** qui visent, d'une part, à actualiser la directive e-commerce du 8 juin 2000 sur la responsabilité des acteurs numériques sur les contenus (haine en ligne, contrefaçon en ligne, vente de produits non-conformes aux normes européennes…) et, d'autre part, à adapter le droit de la concurrence au numérique en mettant en place des mesures ex ante contre les plateformes structurantes (« *gatekeepers* ») et en renforçant les pouvoirs d'enquête pour empêcher le verrouillage d'un marché.

  S'il est nécessaire de renforcer les obligations des services numériques, il est important de ne pas donner trop de pouvoirs à des acteurs étrangers. En effet, la surveillance et le retrait des contenus (haine en ligne, contenus illicites, contrefaçons, produits illicites…) ou la fermeture de comptes ne doivent pas être à la main d'un réseau social ou d'une marketplace qui pourraient outrepasser leurs droits (atteinte à la liberté d'expression, suppression de produits concurrents…), avec un risque de perte de souveraineté.

  Ainsi, si le MEDEF est attaché à la défense d'un internet responsable et considère que les différentes parties prenantes (Etat et opérateurs de plateformes) doivent collaborer pour lutter contre les contenus illicites et rendre Internet plus sûr, le rôle du juge est fondamental pour caractériser les contenus ou produits illicites. En effet, en France, le juge judiciaire est proclamé gardien des libertés fondamentales par l'article 66 de la Constitution et il est donc le seul à pouvoir se prononcer sur l'équilibre entre la nécessité de supprimer des contenus en ligne et la liberté d'expression.

- **S'agissant des enjeux de concurrence et de fiscalité du numérique,** le Medef est en large partie en phase avec les orientations du Gouvernement : nous comprenons parfaitement la recherche d'une plus grande équité fiscale, et donc concurrentielle, entre acteurs « traditionnels » et acteurs « numériques ».

  Bruno Le Maire vient de rappeler dans ses vœux à la presse que la mise en place d'une nouvelle fiscalité internationale répond à l'enjeu de créer des conditions de concurrence équitables, il note que les grands gagnants de la crise actuelle sont les géants du digital. Cela s'inscrit dans la stratégie de reconquête économique nationale du Gouvernement, dans une perspective européenne et internationale. La juste taxation des acteurs du numérique et le « level playing field » sont bien entendu des questions qui participent de la souveraineté économique.

- Il est important du point de vue du Medef d'aboutir à une solution réellement internationale : l'OCDE y travaille depuis plusieurs années et nous contribuons très activement à ces travaux, de façon constructive. Nous

MEDEF

échangeons très régulièrement avec les pouvoirs publics français et l'OCDE, nous faisons valoir nos idées et nos propositions. Nous promouvons une solution multilatérale qui préserve les intérêts des entreprises, qui assure un « level playing field », et qui n'entrave pas la création de valeur et la croissance, et protège les entreprises contre la double imposition.

- Toutefois, au-delà des grandes orientations sur lesquelles nous convergeons avec le Gouvernement, **nous alertons sur la mise en œuvre pratique de la solution OCDE :** les conséquences pour les entreprises françaises pourraient être excessives et contreproductives par rapport aux objectifs poursuivis.

  Nous voulons souligner trois points importants :

  - ✓ la solution envisagée par l'OCDE va bien au-delà de la taxation des seuls géants du numérique : il s'agit en réalité d'une refonte des principes de fiscalité internationale, qui impacterait toutes les grandes multinationales (avec un CA >750 M€) dès lors qu'elles parviennent, grâce aux nouvelles technologies, à s'affranchir de la nécessité de s'implanter physiquement sur un marché local pour atteindre les consommateurs de ce marché. Du fait des mutations technologiques et des nouvelles façons de commercer, le système envisagé par l'OCDE conduit à réallouer une partie du bénéfice taxable à ces pays dits de « consommation ».

    Ce qui veut dire que nos grands champions nationaux – dans le luxe, les cosmétiques, la pharma, etc – seraient impactés. Or, ils s'inquiètent du surcroît de taxation qu'ils pourraient subir.

  - ✓ l'extrême complexité du système proposé par l'OCDE : le risque est celui d'une « usine à gaz » en matière de compliance fiscale pour les entreprises concernées, alors que tous leurs efforts et ressources vont se concentrer sur la résilience et la reprise des activités en sortie de crise.

  - ✓ Les entreprises s'inquiètent également des initiatives que pourraient prendre la Commission européenne prochainement, en cas d'échec des négociations à l'OCDE en 2021 : si l'UE légifère unilatéralement en matière de taxation du numérique, il faut à tout prix éviter une rupture de « level playing field » pour les multinationales européennes par rapport à leurs grandes concurrentes internationales. Ceci est d'autant plus crucial que l'on voit certaines économies, surtout la Chine, sortir très favorablement de la crise sur le plan économique.

En un mot, le Medef rejoint le Gouvernement sur les grandes orientations, mais alerte sur la déclinaison pratique car les conséquences pour les champions français pourraient être préjudiciables, et finalement contraires à la recherche d'une plus forte souveraineté numérique française et européenne.

DOCUMENTS COMPLÉMENTAIRES

Synthèse du rapport de l'Institut des Hautes études du Ministère de l'Intérieur (IHEMI) sur la localisation des données

IHEMI

Synthèse du rapport : La localisation des données personnelle.
Quelle stratégie de sécurité économique pour les intérêts souverains français et européens ?

DONNEES ET ETAT DES LIEUX :

Selon les estimations publiées dans le Digital Economy Compass 2019 de *Statista*, le volume annuel de données numériques créées à l'échelle mondiale a été multiplié par plus de vingt au cours de la dernière décennie. Les perspectives en termes d'évolution sont exponentielles. Les données numériques à caractère personnel sont devenues une source de profit et une matière première qui vaut de l'or. La donnée suscite la convoitise pour ceux qui sont en mesure d'entrevoir le potentiel qu'elle représente. C'est encore plus le cas pour les données de santé et les données industrielles qui offrent des perspectives insoupçonnées en matière d'intelligence artificielle.

Les mégadonnées, l'informatique en nuage et l'internet des objets deviennent donc vite indispensables à la compétitivité, et notamment pour l'Union européenne. Les données sont souvent considérées comme un catalyseur de croissance économique, d'innovation et de conversion au numérique dans tous les secteurs économiques, en particulier pour les PME et la société dans son ensemble. Créées, transportées, exploitées, stockées par des acteurs économiques privés de toute nature, elles ont échappé au contrôle des Etats qui tentent désormais d'en assurer la maîtrise.

Les Etats-Unis d'Amérique, grâce aux GAFAM, se sont vite imposés sur le marché de la donnée personnelle et ont développé un *soft power* couplé à une stratégie d'extraterritorialité juridique agressive. Chine et Russie, dont les sociétés et les systèmes politiques n'ont rien de comparables avec les pays occidentaux, soucieuses de préserver leur souveraineté, ont dans le même temps réussi à bâtir des écosystèmes numériques qui les rendent autonomes mais les coupent chaque jour un peu plus du monde hyperconnecté de l'Internet mondial.

Face à une compétition qui s'apparente à une guerre économique, l'Europe, un géant économique qui peine à s'imposer dans le cloud, construit sa stratégie autour des principes et des valeurs qui lui sont propres. Elle entraîne avec elle des pays d'Afrique, d'Amérique du sud ou d'Asie qui s'inspirent de son RGPD. Consciente d'avoir perdu la bataille des données personnelles, elle construit son arsenal afin de défendre le potentiel extraordinaire que représente son gisement de données industrielles, au travers notamment d'un corpus juridique et du facteur essentiel de la localisation des données.

L'économie mondiale vit sa révolution au travers de la digitalisation. Cette révolution entraîne la naissance de nouveaux espaces, de nouveaux acteurs dont l'activité tourne essentiellement autour de l'exploitation des données numériques. L'ampleur et la rapidité de ces bouleversements offrent des perspectives extrêmement prometteuses pour l'innovation, la croissance et l'emploi. Elles posent aussi aux pouvoirs publics de multiples problèmes allant jusqu'à remettre en question le concept de souveraineté. En effet, la maîtrise de la donnée, en particulier la donnée personnelle, suppose celle des différentes dimensions technologiques du cyberespace divisé en couches physique (le matériel, les systèmes de connexion et de transmission), logique (systèmes d'exploitation, les protocoles de communication, les algorithmes, les applications, etc.), sémantique, cognitive ou informationnelle, loin du concept traditionnel de frontière terrestre.

LES ENJEUX :

Les enjeux géopolitiques et politiques
Le cyberespace est un nouveau monde mais aussi un territoire à part entière où les enjeux de toutes natures sont bien réels. Sa maîtrise requiert le contrôle du réseau physique dont les câbles sous-marins assurent 98 % du flux mondial d'Internet. Gênée par la complexité de sa gouvernance, l'Europe, bien que puissance économique majeure, n'est actuellement pas en mesure de protéger les données générées sur son sol malgré la récente mise en place d'un cadre réglementaire. Ce sont les Etats-Unis qui ont fait main basse sur la gouvernance de l'Internet au travers de leurs lois extraterritoriales dont le Cloud Act. En guise de réponse, la CJCE a invalidé le Privacy Shield en juillet 2020, actant une protection insuffisante

IHEMI

des données personnelles des citoyens européens transitant vers les États-Unis. Ce qui ne dissuada ni Donald Trump de proposer un ultime décret avant de quitter la Maison Blanche, ni l'administration Biden de le valider, décret qui oblige les clouds américains à jouer les espions. L'ingérence des GAFAM dans le projet européen de métacloud GAIA-X, dont l'objectif est de « déGAFAMiser » le cloud européen, montre bien la difficulté de l'Europe à défendre sa souveraineté.

Les enjeux économiques

L'UE et ses 450 millions de citoyens sont un grand producteur de données personnelles et industrielles. Ce marché attractif est colossal : des dizaines de milliers de *data brokers* surfent sur un marché estimé à 169 milliards d'euro en 2020. La publicité digitale est estimée à 620 milliards de dollars en 2021. C'est aussi une manne pour les hackers qui, après avoir piraté un site Internet, revendent les données sur le darknet. Les données personnelles pourraient également devenir une source de revenus pour les internautes qui se voient proposer de revendre leurs propres données. La donnée industrielle devient pour l'Europe un enjeu majeur car elle représente la valeur ajoutée de l'industrie de demain.

Les enjeux démocratiques et sociétaux

Le cyberespace a donné l'opportunité aux GAFAM de disposer des mêmes attributs que les Etats - règlements, monnaie, infrastructures, territoires - et de devenir aussi puissant qu'eux. Certaines puissances n'appréciant pas ce nouvel espace et ce qu'il engendre, ont affiché leur volonté de développer leurs propres réseaux numériques, au service de leurs propres priorités. Les données sont la matière première de la société de l'information et sont de plus en plus utilisées comme un outil d'ingérence par des entités étrangères à des fins politiques, économiques et de déstabilisation, comme l'affaire Cambridge Analytica l'a montré.

Les enjeux technologiques

« Sans souveraineté technologique, pas de souveraineté politique ». Cette maxime a été parfaitement comprise par les États-Unis. Moins par l'Europe. Elle se manifeste par une capacité de stockage qui doit être capable d'absorber les flux colossaux de données et de les transporter, ou encore par les moteurs de recherche et les systèmes d'exploitation. Autant de secteurs dégageant des centaines de milliards de dollars chaque année et en constante augmentation, dominés de la tête et des épaules par les États-Unis.

Les enjeux environnementaux

Stockage, traitement, transport des données engendrent une consommation électrique en constante augmentation qui passerait de 3 % de la consommation mondiale en 2021 à 10 % en 2030. Par ailleurs, ces équipements sont à l'origine de pollutions importantes liées à l'extraction des matières premières indispensables à leur élaboration, leur fonctionnement, ou encore leur traitement en « fin de vie ».

Les enjeux légaux

Les États-Unis ont montré que le droit était vecteur d'hégémonie en promulguant des lois extraterritoriales permettant de s'emparer de données stratégiques, quelle que soit leur localisation dans le monde, pour peu qu'elles soient hébergées par un cloud américain ou par l'une de ses filiales (cf. Cloud Act). De son côté, l'Europe met en œuvre depuis 2016 son propre arsenal juridique mais le combat reste encore inégal. Les normes jouent en outre un rôle majeur dans la conquête de marchés en ce qu'elles permettent notamment d'imposer un standard. Elles facilitent également la réversibilité des données. GAIA-X est un projet européen potentiellement très prometteur qui vise à normer le secteur.

« Code is law » est une manière de signifier que la programmation d'une application, d'un site internet, ou encore que les conditions générales de vente d'un service prennent le pas sur la réglementation. Les géants du net, bien conscients de cette particularité, en usent très largement. Les nouveaux territoires du numérique ont aboli les frontières et rendent les régulations nationales inadaptées.
Pour encourager l'émergence de champions numériques, l'Europe doit prendre modèle sur le Small Business Act américain et encourager ses propres entreprises au travers des marchés publics.

IHEMI

PRÉCONISATIONS ET TRAITEMENT STRATEGIQUE DES RISQUES DU CLOUD EUROPÉEN :

1. Mieux prendre en compte l'importance des normes
La norme donne de la valeur mais ne favorise pas forcément les intérêts des acteurs européens. L'UE doit être plus proactive, participer davantage à l'élaboration des normes, sensibiliser les acteurs publics et privés pour mobiliser les moyens nécessaires et imposer leurs standards au marché.

2. Créer un « Airbus » du cloud européen des données industrielles
L'Europe doit s'appuyer sur ses atouts pour créer un « Airbus de cloud », spécialisé et compartimenté. Pour cela, il convient de mutualiser les commandes publiques, privilégier le vote à la majorité qualifiée et favoriser une synergie public-privé dynamique.

3. Diffuser la culture de protection des données et promouvoir un « consom-acteur » du cloud
L'UE doit imposer l'utilisation d'outils informatiques alternatifs dans les administrations publiques et créer un écosystème partenarial public-privé en subventionnant les applications européennes et en assurant la promotion d'une culture de la protection des données personnelles.

4. Poursuivre et accélérer le renforcement de la réglementation et le soutien aux entreprises
L'UE doit soutenir les entreprises européennes via les marchés publics, dans l'esprit d'un Small Business Act, au travers de la mise en application rapide de textes et règlements (DSA, DMA, DGA), afin de garantir sa souveraineté numérique et la protection de la donnée personnelle du citoyen européen.

5. « Ne pas laisser aux codeurs le soin de choisir nos valeurs » (Lawrence Lessig)
Capable d'influencer le degré de protection de la vie privée ou l'accès à l'information, sans avoir la légitimité issue du processus démocratique, le code informatique crée de facto du droit. Il nécessite une appropriation afin d'offrir aux instances européennes la capacité d'opérer les meilleurs choix.

6. Réduire les entraves politiques pour imposer le label européen des données
En intensifiant sa diplomatie numérique et en adoptant une posture unifiée dans les instances normatives, l'UE doit définir clairement la notion « d'entreprise européenne » et de « localisation européenne des données » pour l'hébergement de ses données personnelles et surtout industrielles.

7. Garantir l'accès aux câbles sous-marins pour éviter le monopole des géants de la Tech
Face à la prédation des entreprises américaines ou chinoises, il s'agit de garantir l'accès aux câbles, en sachant préserver le savoir-faire stratégique en matière de fabrication et de pose, sous peine de se voir imposer une vitesse de flux différenciée ou de voir les contenus filtrés.

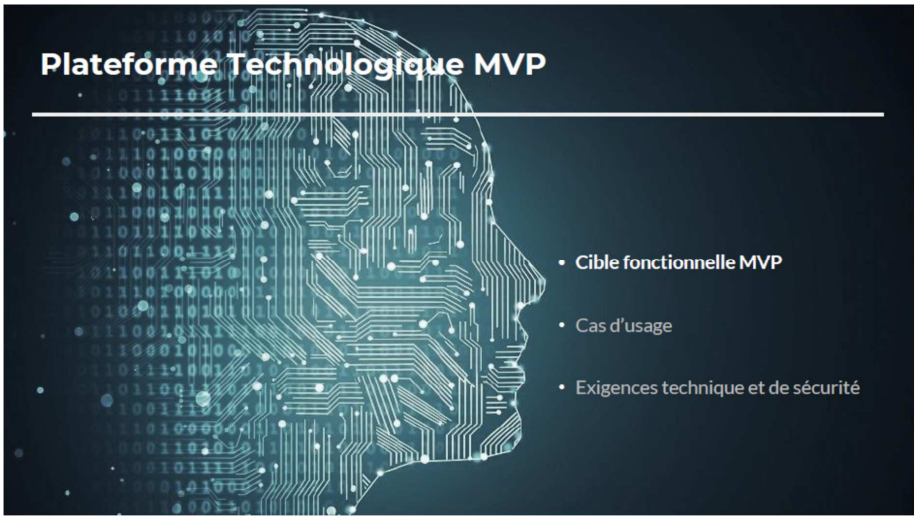
8. Développer la recherche et les savoir-faire européens pour éviter un dépassement de l'UE
En investissant 8 milliards d'euros d'ici 2027, l'Europe doit rester dans la course. Elle en a les moyens, que ce soit dans le domaine spatial (socle des projets Govsatcom et Quantum Communication Infrastructure), la technologie 6G (projet Hera-X), la technologie quantique (projet Quantum Internet Alliance et OPENQKD), le Edge Computing.

9. Promouvoir une approche plus respectueuse de l'environnement et en faire un avantage
L'Union européenne doit poursuivre et favoriser les initiatives en faveur d'un numérique vert (énergie décarbonée, réutilisation du surplus de chaleur...), et encourager la sobriété numérique tant privée que publique.

10. Engager la bataille des données industrielles
Après la prise de conscience et l'impulsion politique donnée au niveau européen par Thierry Breton, l'Union européenne doit tirer parti de ses atouts en matière de données industrielles.

11. Risque systémique : ces préconisations prémuniront contre le « too big to fail » des GAFAM.

Health Data Hub, Besoins fonctionnels, exigences techniques et de sécurité


Plateforme Technologique MVP
• Cible fonctionnelle MVP
• Cas d'usage
• Exigences technique et de sécurité

Vue d'ensemble des objectifs métiers du MVP

Mettre à disposition des porteurs de projet un environnement technologique sécurisé permettant de réaliser les projets pilotes

Mettre à disposition d'un panel d'utilisateurs test un premier catalogue de données accessibles à la demande selon la gouvernance Hub

Tester les fonctions d'administration et de suivi de l'offre de service du Hub

Profils utilisateurs

Porteurs de projets pilotes

Utilisateurs cible MVP : ~20

- Niveau de compétences techniques :
  - Data : Statistiques, code, création d'algorithmes
- Usages :
  - Traitement de la donnée
  - Tests et exécution d'algorithmes
- Principales attentes :
  - Accès à la donnée
  - Outils de traitement, analyse et visualisation à l'état de l'art
  - Puissance de calcul

Utilisateurs de l'offre de service « Catalogue de données à la demande »

Utilisateurs cible MVP : ~50

- Niveau de compétences techniques :
  - Data : Statistiques, code, création d'algorithmes
  - Data : création de clés d'appariement
- Usages :
  - Consultation des données
  - Traitement de la donnée
  - Tests et exécution d'algorithmes
- Principales attentes :
  - Accès à la donnée
  - Outils de traitement, analyse et visualisation à l'état de l'art
  - Puissance de calcul

Administrateurs du « Hub »

Utilisateurs cible : ~5

- Niveau de compétences techniques :
  - Data : appariement (matching probabiliste ou déterministe)
  - Hub : Suivi technique des composants
- Usages :
  - Appariement
  - Gestion technique, administrative et financière du Hub
- Principales attentes :
  - Interface de gestion complète (technique, financière et admin)
  - Interface d'appariement des bases de données

User Stories
Porteurs de projet pilote (1/2)

Usage

- Je dispose d'un « **espace projet** » dédié préparé par l'équipe du Hub présentant en lecture les jeux de données « source » de mon projet, pour lesquels j'ai reçu une habilitation, et selon le(s) moyen(s) de stockage de mon choix (fichier plat, base relationnelle, clef valeur, colonne, document, graphe) :
  - Vues sur les bases de données présentes au catalogue du Hub ;
  - Jeux de données appariés réalisés spécifiquement pour le projet par l'équipe Hub ;
  - Jeux de données propriétaires complémentaires spécifiques au projet, fournis par le porteur de projet à l'équipe Hub.

- Je dispose sur mon « espace projet » **d'outils de requête, d'analyse, de visualisation et de développement** permettant à partir de mes jeux de données « sources » :
  - De créer de nouvelles tables ou jeux de données enrichis sur le moyen de stockage de mon choix, qui viendront automatiquement s'ajouter à mon espace projet ;
  - De réaliser des traitements statistiques ou d'entrainer des modèles de machine learning, en utilisant des librairies de références ;
  - De visualiser un jeu de donnée au moyen d'un outil de data visualisation ;
  - De définir, d'enregistrer et d'exécuter une séquence automatisée de traitements (« pipeline », « workflow ») ;
  - D'importer, d'enregistrer et de gérer différentes versions des algorithmes que je souhaite exécuter.

- Je dispose sur mon « espace projet » d'une **capacité de stockage** (standard, rapide) **et de calcul** (CPU, GPU) garantie dimensionnée à mon besoin, définie en lien avec un expert de l'équipe du Hub et allouée par cette dernière.

User Stories
Porteurs de projet pilote (2/2)

Usage

- J'ai la garantie que l'ensemble des jeux de donnés crées au sein de mon « espace projet » et les algorithmes développés ne sont **accessibles** qu'aux **administrateurs** du Hub et **utilisateurs autorisés** pour le projet.

- J'ai la possibilité depuis mon « espace projet » **d'exporter les commandes et les résultats obtenus** sur l'interface de requête. Cet export peut être **limité en volume** (X Mo) et **en fréquence** (à définir) et est sujet à une approbation explicite de l'administrateur du hub, il est **conditionné par une confirmation** me rappelant :
  - Les conditions d'usage des données du Hub, et en particulier l'interdiction d'exporter des données non anonymes non agrégées ;
  - Mes responsabilités personnelles concernant la protection de ces données individuelles et les conséquences pénales et légales encourues en cas de défaut ;
  - La traçabilité complète de mes opérations et la réalisation d'audit réguliers sur les exports par les équipes du Hub.

- J'ai à ma disposition des API, connectées via un VPN Ipsec, me permettant de :
  - Déclencher des « pipelines »
  - D'exposer des données anonymisées

User Stories
Utilisateurs de l'offre de service (1/3)

Usage

- J'ai accès à un **espace « utilisateurs »** présentant les différents **« espaces projets »** auxquels je suis rattaché et un rappel de leur finalité

- J'ai accès à un **catalogue des jeux de données « publics »** disponibles sur le Hub. Ce catalogue présente :
  - Les jeux de données « publics » disponibles ;
  - Une information sur la structure et le contenu des jeux de données disponibles : champs, couverture, profondeur d'historique, niveau de qualité, fréquence de mise à jour ;
  - Un accès en téléchargement à une documentation publique ;
  - Un accès en téléchargement à un échantillon anonymisés et/ou synthétique des données.

- J'ai accès à un **formulaire mail prérempli** me permettant de formuler ma **demande d'habilitation**. Ce formulaire m'indique les pièces à fournir et les procédures à suivre.

User Stories
Utilisateurs de l'offre de service (2/3)

Usage

- Je dispose d'un ou plusieurs « espace projets » préparés par l'équipe du Hub présentant une vue en lecture des jeux de données « source » du catalogue sur le périmètre sur lequel j'ai obtenu une habilitation pour le projet et la finalité déclarée.

- Je dispose sur mon « espace projet » **d'outils de requête, d'analyse, de visualisation et de développement** permettant à partir de mes jeux de données « sources » :
  - De créer de nouvelles tables ou jeux de données enrichis sur le moyen de stockage de mon choix, qui viendront automatiquement s'ajouter à mon espace projet ;
  - De réaliser des traitements statistiques ou d'entrainer des modèles de machine learning, en utilisant des librairies de références ;
  - De visualiser un jeu de donnée au moyen d'un outil de data visualisation ;
  - De définir, d'enregistrer et d'exécuter une séquence automatisée de traitements (« pipeline », « workflow ») ;
  - D'importer, d'enregistrer et de gérer différentes versions des algorithmes que je souhaite exécuter.

- Je dispose sur mon « espace projet » d'une **capacité de stockage** (standard, rapide) **et de calcul** (CPU, GPU) garantie dimensionnée à mon besoin, définie en lien avec un expert de l'équipe du Hub et allouée par cette dernière.

User Stories
Utilisateurs de l'offre de service (3/3)

Usage

- J'ai la garantie que l'ensemble des jeux de donnés crées au sein de mon « espace projet » et les algorithmes développés ne sont **accessibles** qu'aux **administrateurs** du Hub et **utilisateurs autorisés** pour le projet.

- J'ai la possibilité depuis mon « espace projet » **d'exporter les commandes et les résultats obtenus** sur l'interface de requête. Cet export est **limité en volume** (X Mo) et **en fréquence** (à définir) et est **conditionné par une confirmation** me rappelant :
  - Les conditions d'usage des données du Hub, et en particulier l'interdiction d'exporter des données non anonymes non agrégées ;
  - Mes responsabilités personnelles concernant la protection de ces données individuelles et les conséquences pénales et légales encourues en cas de défaut ;
  - La traçabilité complète de mes opérations et la réalisation d'audit réguliers sur les exports par les équipes du Hub.

User Stories
Administrateurs du « Hub » (1/2)

Usage

- Je peux **ajouter, retirer et modifier des utilisateurs** et leur **attribuer un accès** à la plateforme.

- Je peux **ajouter, retirer et modifier des « espaces projets »** pour lesquels je peux spécifier :
  - La finalité déclarée du projet ;
  - Les utilisateurs habilités à accéder à l'espace projet ;
  - Les outils mis à disposition sur l'espace projet ;
  - La capacité de calcul (CPU, GPU) et de stockage maximum affectée au projet ;
  - Les fichiers, jeux de données ou champs visibles en lecture en tant que jeux de données « source » du projet.

- J'ai accès à un **catalogue** présentant l'ensemble des **jeux de données** présents sur la plateforme, leurs **métadonnées** et les espaces projets y ayant accès. Je peux apposer des marques (« **tags** ») au niveau des fichiers, des métadonnées et des champs, par exemple pour spécifier **des restrictions particulières** concernant l'accès à la donnée. En particulier, je peux apposer une marque pour indiquer les jeux de données qui seront présentés au catalogue de jeux de données « publics ».

User Stories
Administrateurs du « Hub » (2/2)

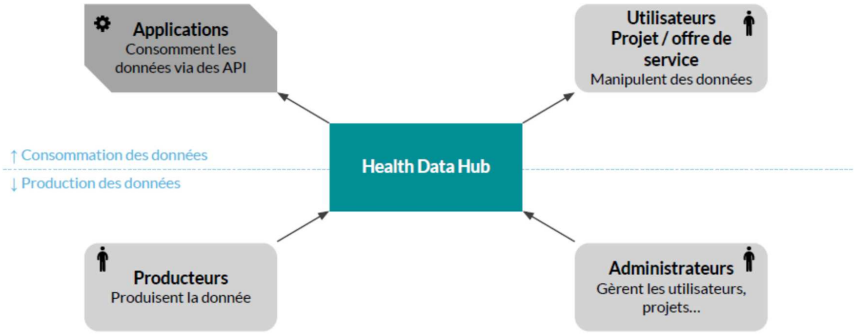
Usage

- Je dispose **d'une interface de supervision unique** couvrant l'ensemble des composants de la plateforme. Elle permet :
  - De suivre la consommation technique (ressources de calcul et de stockage) et financière d'ensemble et par projet ;
  - D'accéder aux interfaces d'administration de l'ensemble des composants (infrastructure, socle applicatif) ;
  - De suivre l'état de la plateforme et de disposer d'un historique des pannes et des opérations de maintenance prévues.

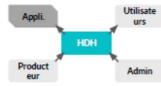
- Je dispose d'un **outil de collecte et d'analyse des journaux** qui me permet de trier, d'ordonnancer et de filtrer en fonction de différents critères l'ensemble des événements du système (authentification, gestion des comptes et des droits, accès aux ressources, modification des stratégies de sécurité, activité des processus, activité des systèmes). En particulier je peux :
  - Disposer d'un visibilité complète sur tous les exports réalisés dans la journée pour réaliser un audit quotidien ;
  - Déterminer pour une période donnée les actions menées par un utilisateur donné ou les utilisateurs ayant procédé à une action données ;
  - Lister tous les événements associés à chacun des objets visualisés et générer des alarmes selon le paramétrage de mon choix.

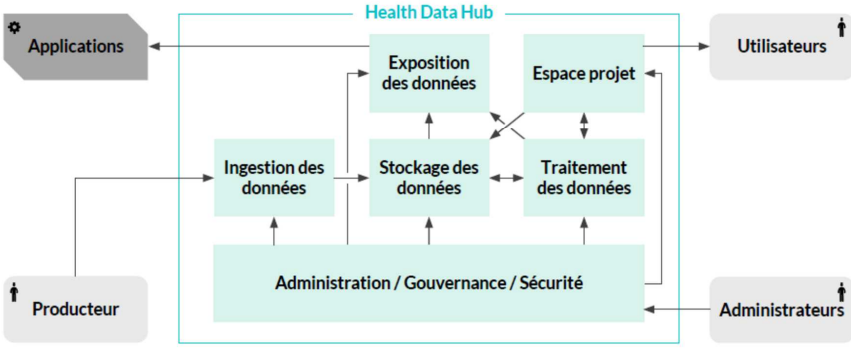
- Je dispose d'un **espace, de capacité de calcul et de stockage et d'outils de traitement de la donnée cloisonnés physiquement du reste de l'infrastructure** me permettant de **réaliser les opérations d'appariements**.

Cible fonctionnelle
Schéma d'ensemble

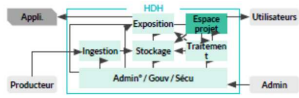


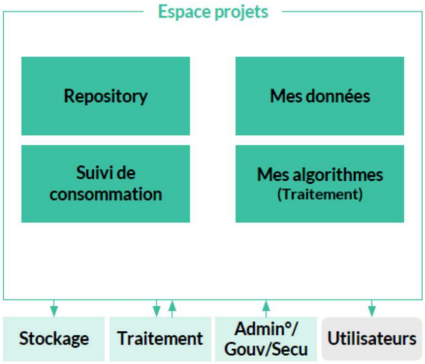
Cible fonctionnelle
Focus : Health Data Hub





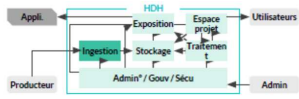
Cible fonctionnelle
Focus : Espace projets

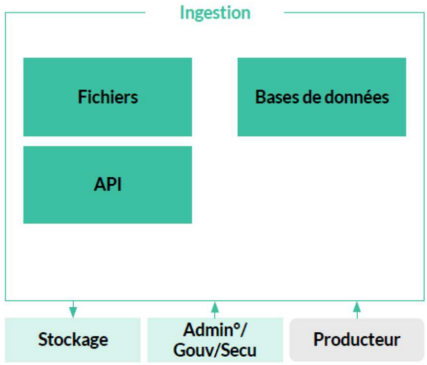




- **Repository**
  - Données propres aux utilisateurs : codes, fichiers, librairies…
  - Historique des exports de données
- **Mes données**
  - Vues sur les données calculées et catalogues de données disponibles pour l'utilisateur
- **Suivi de consommation**
  - Suivi des consommations par projet en volume et temps de calcul
- **Mes algorithmes**
  - Notebook
  - Codes sources

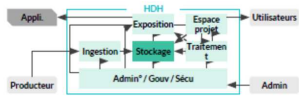
Cible fonctionnelle
Focus : Ingestion des données

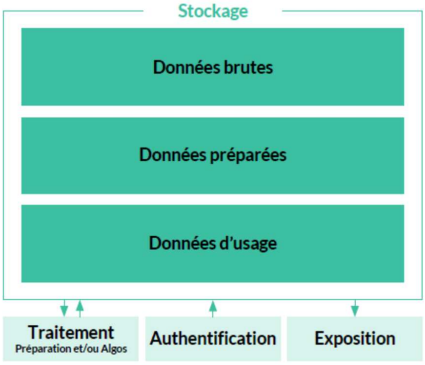




- **Fichiers**
  - Tout type de fichiers (Images, texte, audio, vidéo…)
- **Bases de données**
  - Bases relationnelles
- **API**
  - Mise à disposition d'une API pour permettre aux producteurs de déposer de la donnée

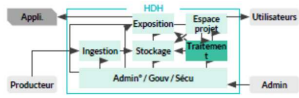
Cible fonctionnelle
Focus : Stockage des données

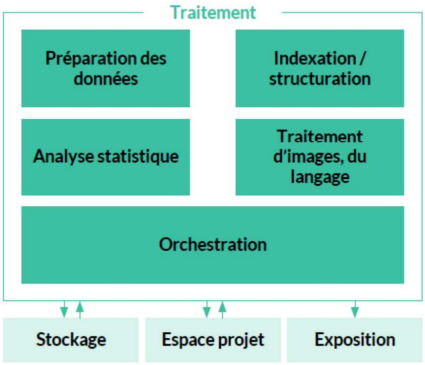




- **Données brutes**
  - Données issues d'une source non modifiées pour rejeu si besoin
- **Données préparées**
  - Données nettoyées, ajout de colonnes afin de répondre a des cas d'usages
- **Données d'usage**
  - Données à destination de l'utilisateur pour faire ses agrégations, statistique ou recherche

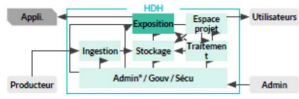
Cible fonctionnelle
Focus : Traitement des données

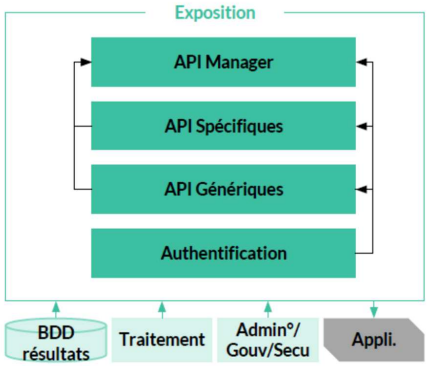




- **Préparation des données**
  - Nettoyage
  - Feature engineering
- **Indexation / structuration**
- **Analyse statistique**
  - Calculs distribués
  - Machine learning
  - Requêtes statistiques
- **Traitement d'images, du langage**
  - Deep learning
- **Orchestration**
  - Gestion du pipeline des traitements

Cible fonctionnelle
Focus : Exposition des données

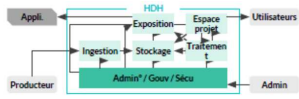


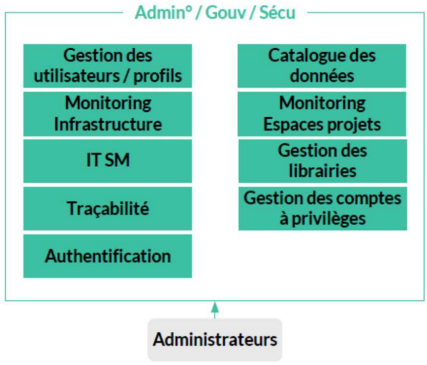


- **API Manager**
  - Exposition des API de manière sécurisée
- **API Spécifiques**
  - API développées sur mesure pour/par les projets
- **API Génériques**
  - API standards sur étagère
- **Authentification**
  - Propagation d'authentification de l'usager auprès des API
  - Validation des droits

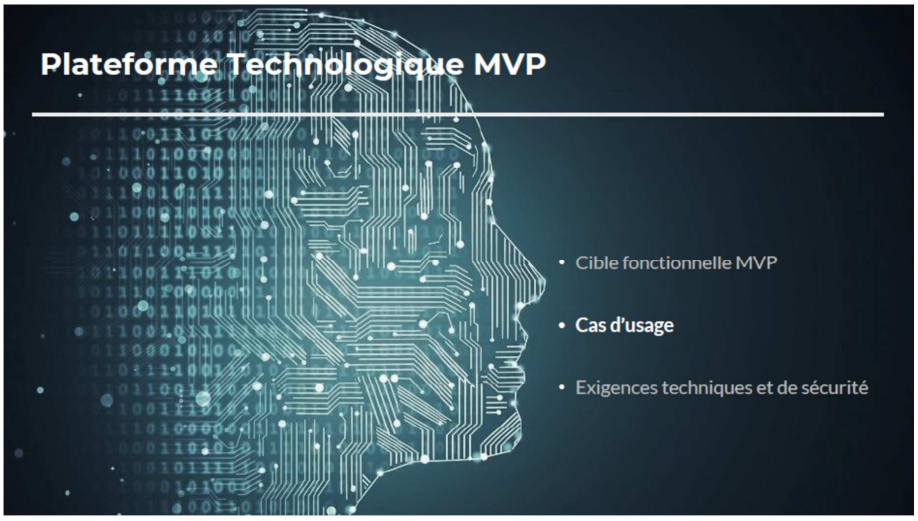
⚠ **On interdit l'exécution de requêtes directement sur le cluster**

Cible fonctionnelle
Focus : Admin°/Gouvernance/Sécurité





- **Gestion des utilisateurs / profils**
  - Ajouts / retraits d'utilisateurs
  - Gestion des droits
- **Catalogue de données**
  - Gouvernance de la donnée
  - Administration des catalogues de données : niveaux d'accès
- **Monitoring Infrastructure**
  - Tableau de bord de suivi et consommation des composants
- **Monitoring des espaces projets**
  - Tableau de bord de suivi et consommation des projets
- **IT System Management**
  - Suivi, traçabilité des demandes et incidents
- **Gestion des librairies**
  - Gestion des versions et catalogues de librairies (jar, ...)
- **Traçabilité**
  - Consultation des logs
  - Génération d'audit
- **Gestion des comptes à privilèges**
  - Gestion des super utilisateurs
- **Authentification**
  - Gestion des protocoles d'identification des utilisateurs


Plateforme Technologique MVP
• Cible fonctionnelle MVP
• Cas d'usage
• Exigences techniques et de sécurité

Exemple de cas d'usage : cas d'usage n°1

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Démontrer le lien entre l'exposition aux antibiotiques et la survenue d'une pathologie définie : • Décrire l'épidémiologie détaillée • Analyser le lien à l'échelle de l'individu et temporo-spatial à l'échelle des populations	**Base résultant de l'appariement des bases suivantes :** • **Entrepôt de données de santés codé avec la pathologie identifiée :** ○ Volume 2To ○ Description : données administratives, sociales et médicales, recueillies lors des consultations et hospitalisations, des patients soignés dans les hôpitaux • **SNDS** ○ Volume : non défini ○ Données extraites du SNDS, selon les critères d'appariement **> Besoin en stockage final** : non défini	• **Traitement** ○ Analyses descriptives, modélisations temporelles, modèles mathématiques. • **Langage** ○ R ○ Python • **Outils** ○ Données scannées : OCR, NLP

Exemple de cas d'usage : cas d'usage n°2

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Identifier des interactions médicamenteuses bénéfiques ou délétères chez des patients atteints d'une pathologie définie : • Identifier les combinaisons médicamenteuses délétères nécessitant la mise en place d'alertes de pharmacovigilance • Identifier les combinaisons médicamenteuses bénéfiques justifiant de la réalisation d'essais cliniques de «repositionnement» de médicaments	**Base résultant de l'appariement des bases suivantes :** • **SNDS** : ○ Volume : 1 à 2 To ○ Données extraites du SNDS, selon certains critères, représentant environ 750 tables par patient. Le nombre approximatif de patients attendu est de 500 000. • **Données patients porteurs** : ○ Volume : 5 Go ○ Description : Dossier médicaux ○ Données stockées sous forme d'une matrice texte. ○ Possibilité éventuelle d'intégrations à faire avec données étrangères **> Besoin en stockage final** : 8 To	• **Traitement** ○ Analyse statistique ○ Approches machine learning pour structurer données – et traitement du langage naturel • **Outils** ○ Bureau virtuel, ○ Serveur R studio ○ Outils de machine learning

Exemple de cas d'usage : cas d'usage n°3

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Créer une base de données rassemblant un set de données minimum pour l'étude de pathologies rares définies : • Déterminer une série d'indicateur de santé publique: prévalence, incidence, typologie des maladies, éléments sur l'histoire des maladies et des parcours des patients • Déterminer autant que possible l'errance diagnostique pour certaines pathologies Les données du SNDS permettront de retracer la totalité du parcours médical des patients et de réaliser des études médico-économiques	**Base résultant de l'appariement des bases suivantes :** • **SNDS** ○ Volume : non défini ○ Données extraites du SNDS, selon les critères d'appariement • **Base de données sur les pathologies étudiées** ○ Volume : 0,2 To ○ Description : environ 30 tables provenant de grands hôpitaux/CHU **> Besoin en stockage final** : 1 To	• **Traitement** ○ Analyse statistique ○ Création d'indicateurs de santé publique • **Langage** ○ R ○ Python • **Outils** ○ Jupyter ○ R studio

Exemple de cas d'usage : cas d'usage n°4

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Etudier l'impact d'une pathologie sur la génèse d'une autre : • Chainer des cohortes rassemblant les données cliniques, biologiques radiologiques et génétiques de ces patients • Analyser l'évolution du parcours de soins à partir d'hypothèses établies sur les données cliniques ou biologiques • Faire émerger des liens de causalité (inférence causale) voire de nouvelles hypothèses de prise en charge, grâce aux approches de machine learning	**Base résultant de l'appariement des bases suivantes :** • **SNDS** ○ Volume : 10To ○ Description : Extraction d'une cohorte • **Données de deux cohortes** ○ Volume : 0.1 To ○ Données épidémiologiques, cliniques, anatomo-pathologiques structurées ○ Données génétiques structurées ○ 40 tables, 900 millions d'entrées **> Besoin en stockage final** : 10 To	• **Ingestion** ○ Ingestion de la base depuis un disque externe • **Traitement** ○ Analyse statistique ○ Machine Learning • **Langage** ○ Python • **Outils** ○ Spark-Scala-Python ○ Jupyter

Exemple de cas d'usage : cas d'usage n°5

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Analyser des images enrichies et créer un modèle prédictif de réponse aux thérapies • Identifier les marqueurs de réponse ou non réponse aux traitements • Identifier les marqueurs de toxicité médicamenteuse	**SNDS** ○ Volume : Non défini ○ Description : Extraction d'une cohorte **Entrepôt de données** ○ Volume : 10 To ○ Description : Données structurées code diagnostics, Traitements, Informations patient, images et compte rendus textuels, tumeurothèque **> Besoin en stockage final** : > 30 To	• **Ingestion** ○ ETL pour les données structurées (cliniques, annotation) • **Traitement** ○ Analyse statistique ○ Machine Learning • **Langage** ○ Python • **Outils** ○ Serveur R studio ○ Jupyter Python, TensorFlow, Keras ○ Module de text mining pour l'annotation automatique à partir des compte rendus textuels

Exemple de cas d'usage : cas d'usage n°6

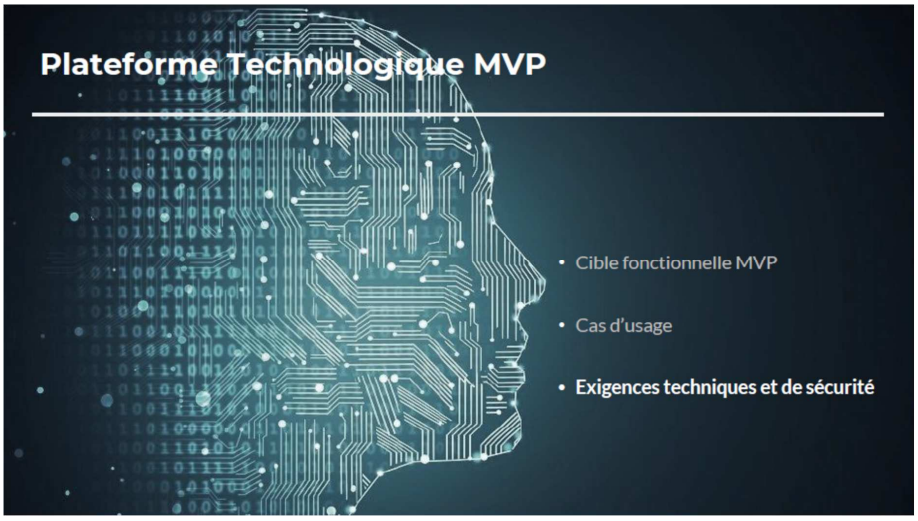
Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Proposer un framework pour l'intégration et l'enrichissement de données hétérogènes • Développer une méthodologie et un algorithme de TAL (traitement automatique du langage) pour traiter les comptes rendus médicaux et extraire les concepts médicaux pertinents • Lancer des cas d'usages médicaux concrets Les données du SNDS permettront de consolider une vision sur l'ensemble du parcours du patient, de limiter les efforts d'annotation et d'évaluer la validité des données extraites.	**Base résultant de l'appariement des bases suivantes :** • **SNDS** ○ Volume : Non défini ○ Description : Données extraites du SNDS, selon les critères d'appariement • **Entrepôt de données** ○ Volume : 0,5 To ○ Description : données textuelles de rapports médicaux partiellement structurées, totalité des Comptes Rendus disponibles : entre 20-30 millions **> Besoin en stockage final** : 1 To	• **Traitement** ○ Analyse statistique ○ NLP • **Langage** ○ Python • **Outils** ○ Serveur Jupyter

Exemple de cas d'usage : cas d'usage n°7

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Etudier les facteurs influençant les choix entre deux types d'allocations pour personnes handicapées en termes de coûts, de contenus des plans d'aide, de restes à charge, etc. **Mettre en œuvre des techniques d'appariement innovantes**, sur la base d'informations identifiantes : nom, prénom(s), date de naissance, adresse postale, mais non du NIR	**Base résultant de l'appariement des bases suivantes :** • **Base 1** ○ Volume : 10 Go ○ Description : données structurées au format SAS, nombre d'observations : 1 300 000 • **Base 2** ○ Volume : 10 Go ○ Description : données structurées au format SAS, nombre d'observations : 120 000 **> Besoin en stockage final** : 1 To	• **Traitement** ○ Analyse statistique • **Langage** ○ Python • **Outils** ○ Serveur R studio

Exemple de cas d'usage : cas d'usage n°8

Finalité du cas d'usage	Données à traiter	Traitement requis et outils
Concevoir des algorithmes d'Intelligence Artificielle (IA) pouvant aider des équipes médicales dans leur pratique quotidienne d'imagerie, et ainsi contribuer à encore davantage populariser la technique en facilitant son utilisation afin d'améliorer les soins. **L'enjeu médical est de développer et évaluer des algorithmes d'IA** détectant différents organes et leurs lésions	• **Données d'imagerie d'hôpitaux :** ○ Volume : Non défini ○ Description : images (nombre : 1 440 000) et comptes rendus (format DICOM et TXT) **> Besoin en stockage final** : 4 To	• **Ingestion** ○ Copie des données par disques USB cryptés • **Traitement** ○ Extraction automatique de contenu dans les comptes rendus: NLP ○ Machine Learning : apprentissage supervisé, semi-supervisé et non supervisé : détection et segmentation d'organes et de pathologies dans des images 2D, génération d'images de synthèse • **Langage** ○ Python • **Outils** ○ Image processing et visualisation ○ API permettant de se connecter aux bases de données


Plateforme Technologique MVP
• Cible fonctionnelle MVP
• Cas d'usage
• Exigences techniques et de sécurité

Exigences techniques et de sécurité
Infrastructure et maintenance

Brique	Principales exigences
Infrastructure	Hébergeur agrée ou certifié "Hébergeur de données de santé" > Quelle couverture sur l'offre de service ?
	[SNDS] Territorialité : France
	Possibilité d'utiliser des CPU et des GPU comme capacité de calcul (y compris sur domaine HDS)
	Accès à des supports de stockages rapides (SSD ou mémoire flash) ou standards
	Elasticité : capacité d'accueil d'une centaine nŒuds sans modification autre qu'une configuration et sans impact sur la performance du système
	Capacité de tag des objets cloud en vue d'une intégration dans un référentiel d'entreprise (ITSM)
	Le format des données en fin de contrat doit être exploitables et permettre une récupération des données (préciser média et coût)
	Taux de disponibilité minimum : 99,95%

Exigences techniques et de sécurité
Bureau Virtuel, Plateforme Data : sujets transverses, ingestion

Brique	Principales exigences
Bureau Virtuel	Solution VDI avec capacité à customiser les bureaux virtuels
	Capacité à capturer le keylogger et de la capture vidéo sur sessions VDI
	Partage de l'annuaire d'authentification entre le hub et la plateforme VDI
Plateforme Data - Transverse	Système d'exploitation avec un support valide de la part d'un éditeur ou d'un prestataire de service.
	Possibilité d'exposer des données par le développement d'API spécifiques
Plateforme Data – Ingestion / Echanges	Broker de messagerie asynchrone
	Ingestion Batch / Micro-batch

Exigences techniques et de sécurité
Plateforme Data : moyens de stockage

Brique	Principales exigences
Plateforme Data – Moyens de stockage	Moyen de stockage en cache
	Moyen de stockage objet
	Moyen de stockage distribué
	Moyen de stockage structuré : base relationnelle
	Moyen de stockage structuré : base clef-valeur
	Moyen de stockage structuré : base orientée colonne
	Moyen de stockage structuré : base orientée document
	Moyen de stockage structuré : base orientée graphe
	Moteur de recherche

Exigences techniques et de sécurité
Plateforme Data : Traitement de la donnée

Brique	Principales exigences
Plateforme Data – Traitement	Moteur de calcul distribué pour les traitements en batch
	Moteur de calcul distribué pour les traitements en flux
	Moteur d'exécution d'applications conteneurisées
	Moteur de calcul distribué pour l'apprentissage automatique supportant le calcul sur GPU
	Calcul non distribué dans un container pour les data set de faible volume

Exigences techniques et de sécurité
Plateforme Data : Usages

Brique	Principales exigences
Plateforme Data – Usages	IDE Python
	IDE R
	L'import de librairies extérieures (Datascience / Machine Learning de référence (Tensorflow, Keras, Sci-kit, Pandas, Theano…)) peut se faire online via un nexus synchronisé avec l'extérieur, miroir de cran ou pip, ou en en offline en important les librairies dans un repository Git
	Outil de data visualisation : quelles solutions sur étagère vs solutions dans la market place (SAS, R Studio…) ?
	Système de contrôle des versions, gestion de code source, jalons, anomalies
	Outils Devops (SonarQube, Jenkins)

Exigences techniques et de sécurité
Sécurité

Brique	Principales exigences
Sécurité	Authentification forte (selon les exigences du palier 2 - PGSSI-S) cascadée sur toutes les couches de la solution
	Certificat management ayant la capacité d'importer des PKI d'entreprises externes et certifié critères communs > Quelle étendue de l'application des critères communs sur l'ensemble de l'offre de service ?
	Gestion des accès à la donnée selon les droits attribués à l'utilisateur et les politiques définies au niveau fichier, méta-données, champs
	Journalisation complète des activités (voir palier 3 de la PGSSI-S ci après), y compris celles des administrateurs, sur tous les niveaux de profondeur de l'infrastructure et des applicatifs
	Possibilité de transmettre quotidiennement des traces vers une infrastructure extérieure à celle du hub
	Scellement quotidien des traces et transmission de la preuve de scellement à un tiers de confiance
	Solution d'exploitation et d'analyse des traces
	Dispositif de détection d'intrusion et d'attaques
	Possibilité de génération d'audit
	Fonctionnalité de chiffrement des données sensibles
	Liste des certifications de sécurité et conformité

Exigences techniques et de sécurité
Gouvernance de la donnée, administration / supervision

Brique	Principales exigences
Gouvernance de la donnée	Catalogue de données, tagging des fichiers, des méta-données, des champs
	Gestion du cycle de vie de la donnée : planification de l'alimentation, des traitements, du stockage, de l'archivage, et durée de rétention
Administration / Supervision	Ajout, retrait et modifications des utilisateurs, définition des droits et profils qui conditionnent les accès, définition d'un role base access
	Allocation et suivi des ressources (CPU, RAM, GPU) affectées à un utilisateur ou un traitement
	Administration et suivi de l'intégralité des composants de la plateforme depuis une interface de supervision unique

Exigences techniques et de sécurité
Prestations : Conception et intégration, Sécurité

Brique	Principales exigences
Conception et intégration	Définition de l'architecture technique et fonctionnelle cible du MVP
	Définition de la stratégie et du plan de test
	Installation, configuration, sécurisation et test de la plateforme
	Transfert de connaissances et accompagnement
Sécurité	Maintien en condition de sécurité et application des correctifs > Couverture dans le cas de la consommation d'un service IAAS
	Maintien en condition de sécurité et application des correctifs > Couverture dans le cas de la consommation d'un service PAAS

Focus : Authentification forte et PKI
Exigences

- En matière d'authentification, le SNDS impose d'être conforme aux exigences du palier 2 du Référentiel d'identification de la PGSSI-S : soit une authentification forte à multi facteurs.
- De plus, la PGSSI-S, indique que pour ce dispositif, l'utilisateur voulant accéder au système, utilise une bi-clé d'authentification (couple clé privée, clé publique) en provenance d'une PKI.
- La solution devra être un service sécurisé et résilient qui utilise des modules de sécurité matérielle validés **critères communs** pour protéger les clés.
- Les clés privées seront gérées et stockées par le ministère, le certificat management doit donc avoir la capacité d'importer des PKI d'entreprises externes
- Les journaux de toutes les utilisations clés devront être mis à disposition afin de répondre aux besoins en matière de réglementation et de conformité.
- Ces journaux devront pouvoir être envoyés vers un service (SIEM: Security Information and Event Management) d'analyse et de détection des menaces.
- Le MVP doit donc disposer de capacités :
  - D'authentification forte
  - De gestion des clés avec importation de PKI d'entreprises externes

Focus : Traçabilité
Exigences

- Les exigences de traçabilité (typologie, profondeur, journalisation) sont fixées par le SNDS et doivent être conformes au **palier 3** d'imputabilité décrit dans la PGSSI-S (détail ci après)

- Des solutions techniques doivent être mises en regard de chacune de ces exigences pour assurer la conformité de plateforme et son homologation. En particulier : Chaque composant applicatif doit journaliser avec l'utilisateur et par conséquent doit permettre l'authentification ou la cascade d'authentification afin de tracer les actions alignée sur les mêmes time stamp. Les logs sont tous remontés dans une console centrale. Il faut prévoir une application pour reconstruire le parcours utilisateurs
  Ex: Le notebook trace la connexion de l'utilisateur et l'exécution de code qui fait une requête à la base de données. La base de données reçoit une requête authentifiée et trace la requête et potentiellement les données (interdiction de réexécuter par la suite).

- Les traces sont transmises quotidiennement vers une infrastructure extérieure au hub

Focus : Traçabilité
Exigences de traçabilité du palier 3 de la PGSSI-S

Prérequis	Génération de piste d'audit	Conservation des traces	Restitution de la piste d'audit	Documentation spécifique
• Palier 1 du référentiel d'identification et d'authentification • Gestion dans le temps des identités, des rôles et des habilitations • Heure partagée par l'ensemble des composants du SIS	• Traces fonctionnelles : o type d'action o horodatage o Identité utilisateur o résultat (succès, erreur, refus) o données métiers concernées et traces embarquées (ex: identifiant du document) o version o contexte de réalisation, informations fournies (ex : message d'avertissement) o paramétrage technique de l'application • Traces techniques d'au moins un type de composant : o type d'action o horodatage o identité (utilisateur, machine , programme)	• Possibilité d'extraction des traces pour conservation dans des endroits multiples pour réduire le risque de modifications systémiques • Archives journalières regroupant l'ensemble des traces • Scellement quotidien des traces • Conservation des traces sur une durée glissante de 6 mois	• Outil de gestion permettant : o la restitution ergonomique des traces utilisable par des non spécialistes de la sécurité o la réconciliation des traces autant que de besoin o la gestion d'un format pivot ou gère de nombreux formats de traces • Guide didactique d'utilisation de l'outil de gestion de la preuve	• Documentation des dispositifs d'authentification, de gestion des identités, des rôles, des habilitations et des traces • Description des sources des traces et des processus mis en œuvre de la génération à la constitution de l'archive journalière • Description des processus mis en œuvre de la génération à la réconciliation

Health Data Hub, note sur les conséquences de l'arrêt Schrems II

DLA PIPER

MEMORANDUM

À	Stéphanie Combes, Thomas Duong, Clémence Servigne
De	Health Data Hub / Plateforme des Données de Santé
Sujet	**Analyse de risque de l'utilisation des services d'hébergement de Microsoft par HDH au regard du RGPD**
De	Denise Lebeau-Marianna, Yaël Hirsch (France) Andy Serwin, Katie Lee (US)
Date	10 juin 2021

1. Résumé de notre analyse juridique

Malgré les conditions spécifiques mises en place par HDH pour le traitement des données personnelles sur sa plateforme[1], la CNIL a considéré que le recours à des solutions d'hébergement fournies par des acteurs étasuniens est incompatible avec la décision de la CJUE du 16 juillet 2020 (« Décision Schrems II »), étant donné le risque de transfert potentiel de données traitées en Europe vers les États-Unis en cas d'une demande de communication émanant d'une autorité américaine en vertu des lois de surveillance américaines.

Si le juge des référés du Conseil d'Etat n'a pas exclu un tel risque, il ne relève pas pour autant une violation grave et manifeste du RGPD dans la mesure où les données restent localisées en Europe et a donc autorisé HDH à poursuivre le recours à la solution Microsoft Cloud Azure pendant une période transitoire jusqu'à ce qu'une solution technique alternative soit trouvée, en veillant à mettre en place des mesures supplémentaires.

Après l'ordonnance du Conseil d'Etat du 13 octobre, la CNIL a ainsi pu délivrer des autorisations à plusieurs projets pilotes du HDH qui n'ont pas de lien avec la crise sanitaire actuelle, en estimant que des garanties avaient été apportées en l'espèce sur le recours à un prestataire soumis au droit américain.

[1] *Absence de transferts de données vers les États-Unis, localisation des données en France, absence d'accès aux données par Microsoft Irlande et Microsoft US y compris pour des motifs de support technique, pseudonymisation des données de santé, chiffrement avec les secrets de chiffrement sous le contrôle du HDH et mise en place de mesures contractuelles, techniques et organisationnelles*

DLA PIPER

Face au débat soulevé par la Décision Schrems II et l'ordonnance du Conseil d'Etat, HDH a souhaité savoir si le recours à Microsoft présentait réellement un risque pour les données traitées sur sa plateforme et si des mesures supplémentaires à celles déjà en vigueur étaient nécessaires.

La position très stricte de la CNIL, basée sur la Décision Schrems II, ne semble pas fondée pour les raisons suivantes :

1. **A titre préliminaire, il y a lieu de noter que la Décision Schrems II ne devrait pas s'appliquer au contexte du HDH** :

   ✔ La Décision Schrems II s'applique à un cas de transfert de données entre une société UE, Facebook Irlande, et une société US, Facebook US alors que **dans le cas du HDH, les données de santé sont hébergées en France et ne peuvent être transférées par HDH**, conformément à l'interdiction prévue par le contrat avec Microsoft et l'arrêté ministériel du 9 octobre 2020 ;

   ✔ **Dans l'hypothèse où il y aurait un transfert, celui-ci ne pourrait résulter que de l'initiative de Microsoft**, répondant à une demande éventuelle des autorités dans le cadre des lois américaines de surveillance, sous réserve que lesdites lois soient applicables, une telle application étant peu probable dans le contexte de HDH comme démontré ci-dessous ;

   ✔ **un tel transfert interviendrait alors en dehors du champ d'application des Clauses Contractuelles Type en place** (visé par la Décision Schrems II) **puisqu'en dehors des instructions du HDH**, dès lors le transfert serait réalisé par **Microsoft** en violation de ses obligations contractuelles, et lui confèrerait ainsi la **qualification de responsable du traitement**.

2. **Les conditions d'application des lois de surveillance américaines ne sont pas vérifiées dans le contexte du traitement effectué par HDH** :

   ✔ **En ce qui concerne l'article 702 du FISA :** (i) **il ne permet pas** aux autorités américaines **de procéder à une surveillance ciblée** d'une personne étrangère auprès d'une entreprise située **à l'extérieur des États-Unis** (en dehors du champ de compétence territoriale des tribunaux américains) **;** (ii) de surcroît, **la cible de la surveillance** doit être **une « puissance étrangère » ou « un agent d'une puissance étrangère ». HDH est en France et ne peut pas vraiment être qualifié d'agent d'une puissance étrangère, (iii)** l'activité de la cible doit porter sur le terrorisme international, des activités clandestines de renseignement, la prolifération d'armes etc.). **Or l'activité de recherche dans la santé est bien éloignée de son champ d'application.**

   ✔ **En ce qui concerne le décret présidentiel EO 12333**, celui-ci permet d'exiger la transmission de données même situées en dehors des États-Unis. Néanmoins (i) il

confère à une autorité américaine le **pouvoir de mener des activités de renseignement à condition que ce soit de son propre chef mais ne peut servir de fondement légal pour contraindre une entreprise tierce (ici, Microsoft), ou même HDH à la communication d'informations ;** (ii) il vise par ailleurs "*l'acquisition de renseignements étrangers importants, ainsi que la détection et la lutte contre les activités terroristes internationales, la prolifération des armes de destruction massive et l'espionnage mené par des puissances étrangères* ». **Les données traitées par HDH sont donc clairement en dehors de son champ d'application.**

✔ **Au regard du Cloud Act** (non visé par la Décision Schrems II) : (i) son application nécessite que les **données hébergées** par Microsoft soient en la "***possession, la garde, ou le contrôle***" **de Microsoft**. **Un tel critère ne devrait pas être vérifié si les données de santé sont chiffrées avec des moyens qui restent sous le contrôle du HDH ;** (ii) par ailleurs, le critère de la cible posé par le Cloud Act, qui est « ***d'obtenir la communication de données relatives à des crimes commis aux Etats-Unis*** » ne sera pas non plus satisfait compte tenu de la nature des données traitées par HDH. En outre, la communication des données doit reposer sur un mandat spécifique à la personne visée par l'enquête sur les crimes commis.

3. **Si la Décision Schrems II devait s'appliquer, comme le considère la CNIL, il convient de déterminer si la dérogation de l'article 49 du RGPD fondée sur l'intérêt public** de la nécessité de poursuite des missions du HDH **pourrait servir de base légale au transfert de données potentiel incriminé**.

✔ En effet, la Décision Schrems II a confirmé que l'annulation du Privacy Shield ne laissait pas de vide juridique grâce à l'article 49 du RGPD, qui peut donc servir de base légale pour un transfert vers les États-Unis.

✔ **Cette base légale pour le transfert des données, est reconnue par l'avis de la CNIL du 8 octobre 2020 et par la décision du Conseil d'Etat du 13 octobre 2020, mais de manière restrictive** en justifiant son **application par la** situation spécifique couverte (un groupement reconnu d'intérêt public hébergeant des travaux de recherche dans un contexte de crise sanitaire) qui satisfait ainsi les tests de strict nécessité (urgence sanitaire). Ainsi le bénéfice de cette dérogation pour recourir à la solution Microsoft, nécessite que chaque projet de recherche soit examiné afin de s'assurer, pour chacun d'eux, si le transfert est justifié le temps de la période transitoire par « *les risques sanitaires encourus et appropriée aux circonstances de temps et de lieu, compte tenu, tout à la fois, de l'urgence s'attachant à sa conduite et de l'absence de solution technique alternative satisfaisante permettant d'y procéder dans les délais utiles* »

✔ **Les limites ainsi apportées au bénéfice du recours à la dérogation de l'article 49-1 d) appellent quelques interrogations : (i)** le CEPD indique dans ses guidelines que la dérogation s'applique « *lorsqu'il peut être déduit du droit de l'Union ou du droit de l'Etat membre auquel le responsable de traitement est soumis que ces transferts de données*

sont autorisés pour des motifs importants d'intérêt public », (ii) En l'espèce, nous comprenons que la CNIL et le Conseil d'Etat **ont considéré que la dérogation de l'article 49-1 d) était applicable pour justifier le transfert de manière transitoire du fait de la mission d'intérêt public du HDH reconnue par les textes de droit français** (arrêté du 29 novembre 2019 et Article L1462-1 du code de la santé publique) et de la nécessité de la poursuivre **même si ces transferts ne sont pas explicitement visés par ces textes, ils seraient donc induits par la mission d'intérêt public du HDH** ; (iii) Si ces textes ont servi de base pour appliquer une telle dérogation, on peut s'interroger sur les limites apportées par la CNIL et le Conseil d'Etat pour y recourir puisque les textes de référence n'opèrent pas de distinction entre les différents projets de recherche qui présentent tous une finalité d'intérêt public ; (iv) enfin, l'article 49 du RGPD lui-même n'apporte pas de limites dès lors que les conditions de son application sont satisfaites . En effet, c'est lorsque le transfert **ne peut être fondé sur aucun mécanisme de transfert (y compris les dérogations de l'article 49) qu'un encadrement strict doit être appliqué.**

✔ **On pourrait même s'interroger sur la pertinence de l'application de l'article 49 pour une période transitoire comme préconisé par la CNIL et le Conseil d'Etat** : au regard (i) de sa compatibilité avec l'interdiction de transfert édictée par l'arrêté ministériel du 9 octobre 2020 et (ii) du risque potentiel de transfert dénoncé par la CNIL, lequel ne peut être considéré comme étant à l'initiative de HDH mais de Microsoft. Par conséquent, si le transfert est considéré comme effectué par Microsoft et non HDH, la base légale des motifs importants d'intérêt public n'a pas lieu de s'appliquer.

4. **A la lumière de ce qui précède et de toutes les mesures prises par HDH et Microsoft, HDH est en mesure de démontrer que des précautions supplémentaires ne devraient pas être requises, quelle que soit l'hypothèse retenue :**

✔ **La Décision Schrems II ne s'applique pas** : aucune mesure supplémentaire ne devrait être nécessaire dès lors qu'il n'y a aucun transfert de données grâce aux mesures mises en place par HDH avec Microsoft**. En l'absence de transfert, le risque que les dispositions des CCT ne soient pas respectées dans le pays d'accueil des données (aux Etats-Unis) n'est pas vérifié. Il n'est donc pas nécessaire de les suppléer par d'autres mesures**.

✔ **La Décision Schrems II est considérée applicable** :

- **Si HDH est qualifié de responsable de traitement des transferts (**cette qualification n'étant nullement vérifiée dans les faits comme indiqué au point 1 ci-dessus**), il peut bénéficier de la dérogation de l'Article 49-1 d), dont l'application** selon les recommandations du CEPD[2] et le texte de l'article 49 du RGPD **ne requièrent pas la mise en œuvre de mesures supplémentaires**.

[2] Recommandations 01/2020 du Comité Européen de la Protection des Données (CEPD) du 10 novembre 2020, paragraphe 27

- **Comme démontré ci-dessous, les lois de surveillance américaines n'étant pas susceptibles de s'appliquer, le risque que les CCT ne protègent pas suffisamment les données, si celles-ci font l'objet d'un transfert, devrait être très limité, voire exclu**. En exigeant la mise en œuvre de mesures supplémentaires, l'avis de la CNIL ne suit pas l'analyse au cas par cas requise par la Décision Schrems II **puisqu'elle ne procède pas à une évaluation de l'instrument de transfert en place comme le requiert l'étape 3 des Recommandations du CEPD 01/2020 au regard du caractère effectif de l'application des lois de surveillance mais de leur application potentielle ou hypothétique qui n'est pas vérifiée dans le contexte des traitements de HDH**.
- Etant donné les nombreuses mesures techniques et organisationnelles déjà en place et bien que les mesures contractuelles soient également très complètes, HDH peut, pour continuer de démontrer sa bonne volonté, envisager de les compléter notamment par des dispositions contractuelles visant à : (i) obtenir de Microsoft de conforter le fait que tout risque de transfert est exclu étant donné le caractère spécifique des traitements de HDH, qui rend inopérant le risque soulevé par une applicabilité des lois de surveillance américaines (ii) anticiper les nouvelles dispositions des CCT dès qu'elles seront finalisées par la Commission Européenne.

5. **Enfin, si les lois de surveillance américaines devaient s'appliquer, hypothèse qui reste peu probable, elles entreraient en conflit avec l'Article 48 du RGPD**

✔ **En effet, l'article 48 du RGPD interdit un transfert vers les États-Unis depuis une entité de Microsoft établie en Europe sur le seul fondement d'une demande de renseignement émanant des autorités américaines** et ce indépendamment du fait que le transfert soit réalisé directement depuis Microsoft Irlande ou qu'un tel transfert se fasse par l'intermédiaire de Microsoft US, dès lors que la demande de communication est relative à des données personnelles de personnes physiques situées dans l'Union Européenne.

✔ **En répondant à une telle demande, Microsoft violerait donc le RGPD qu'elle s'est engagée à respecter et ses obligations contractuelles à l'égard du HDH.**

✔ **Pour être valable une telle demande d'une autorité étrangère doit passer par des traités multilatéraux d'entraide mutuelle**, comme exigé par l'Article 48 du RGPD, qui n'existent pas pour l'instant entre la France et les Etats-Unis en matière de renseignements.

Conclusion :

Le risque soulevé d'un transfert vers les Etats-Unis du fait du traitement des données personnelles du HDH en ayant recours à la solution Microsoft ne semble pas justifié après un examen approfondi (i) **du champ d'application des lois de surveillance américaines et des conditions de leur mise en œuvre**, (ii) des **mesures techniques, organisationnelles et**

contractuelles négociées et mises en place par HDH avec Microsoft, (iii) de la **Décision Schrems II** et **notamment des dérogations de l'article 49 du RGPD** qu'elle suggère d'appliquer et enfin (iii) **des dispositions du chapitre V du RGPD régissant les conditions de transfert hors UE**. Par conséquent, HDH ne devrait pas être tenu de mettre des mesures supplémentaires en place, ayant mis en œuvre tout ce qui était possible pour garantir au mieux la protection des données des personnes concernées.

DLA PIPER

2. Rappel du contexte

2.1. Health Data Hub ("HDH"), Plateforme de Données de Santé (PDS), a été créé par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé et un arrêté du 29 Novembre 2019 pour faciliter le partage des données de santé à des finalités de recherche. **HDH est le responsable du traitement des bases de données qu'il héberge de manière pérenne pour répondre à des projets de recherche** et les rend accessibles sous une forme pseudonymisée, par l'intermédiaire d'une plateforme sécurisée. **Les porteurs des projets de recherche restent responsables des traitements qu'ils mettent en place en utilisant les données qui leur sont rendues accessibles par HDH par l'intermédiaire de la plateforme**. Le traitement de données réalisé par un porteur de projet est soumis à l'autorisation préalable de la CNIL ou à son contrôle, laquelle régit donc l'ensemble des conditions de traitement de données réalisés sur la plateforme. Un arrêté spécifique du 10 juillet 2020 a été adopté afin de prescrire les mesures générales nécessaires pour faire face à l'épidémie de Covid-19. Cet arrêté inclut, en son article 30, des dispositions sur les conditions d'utilisation et de conservation des données de santé liées à la pandémie par HDH aux fins de les rendre accessibles à la recherche sur cette maladie. **Cet arrêté a conduit à prioriser l'utilisation de la plateforme HDH, dont le cadre légal n'était pas encore finalisé, pour la recherche sur la Covid-19 et a ainsi modifié le calendrier des projets de recherche** devant être menés par l'intermédiaire de la plateforme HDH.

2.2. **HDH a sélectionné les services d'hébergement cloud de Microsoft dénommés AZURE pour héberger la plateforme**. Le « Contrat » a été conclu avec Microsoft Ireland Operation Limited ("Microsoft" ou « Microsoft Irlande »). **Les données personnelles de santé étaient à l'origine hébergées sur des serveurs situés aux Pays-Bas et sont désormais hébergées en France.** Microsoft agit en tant que sous-traitant. La société mère du groupe, Microsoft Corporation, a son siège social aux États-Unis ("Microsoft US"). Microsoft assure la **protection des flux de données personnelles depuis la France vers les États-Unis** sur **le fondement des Clauses Contractuelles Types de la Commission Européenne de responsable du traitement à sous-traitant** (les « CCT »). HDH a toutefois obtenu de Microsoft, par plusieurs avenants au Contrat, **la garantie qu'aucune donnée de santé ne serait transférée en dehors de l'Union Européenne (UE)**. Les seules données faisant l'objet d'un transfert sont les données de télémétrie pour assurer le bon fonctionnement des services, et, si nécessaire, celles ayant pour objet la facturation. **Par conséquent, aucune donnée de santé ne peut faire l'objet d'un transfert, y compris pour des raisons de support technique.**

2.3. L'Association Le Conseil National du Logiciel Libre (le "CNLL") et autres ont déposé une requête en référé à l'encontre du HDH devant le Conseil d'État, le 28 septembre 2020, aux fins d'obtenir la suspension d'urgence des traitements de données personnelles par HDH au motif que la centralisation des données de santé et les conditions de traitement

mis en œuvre par HDH étaient manifestement illégales et attentatoires au droit à la vie privée et à la protection des données personnelles. Les plaignants ont également sollicité l'avis de la CNIL sur les implications de l'invalidation par la CJUE du Privacy Shield sur les conditions des traitements des données réalisés par HDH.

2.4. **Le 8 octobre 2020, la CNIL a rendu un avis où elle considère, sur le fondement de la décision de la CJUE du 16 juillet 2020** (la « Décision Schrems II »), que quand bien même des mesures seraient prises par HDH (conformément à un avis précédent de la CNIL, en date du 20 avril 2020) pour empêcher Microsoft de transférer des données personnelles vers les États-Unis pour la fourniture des services, **dès lors que Microsoft a son siège aux États-Unis, elle peut être soumise aux lois américaines de surveillance, ce qui peut la conduire à transférer des données personnelles hébergées au sein de l'UE aux autorités publiques américaines.** Un tel transfert et la communication des données en résultant constitueraient une violation de l'article 48 du RGPD et, plus généralement, des dispositions du RGPD régissant le transfert de données personnelles. Par conséquent, **la CNIL a considéré que les services d'hébergement susceptibles d'être soumis aux lois américaines de surveillance sont illégaux.** Elle en a déduit que les conditions d'hébergement doivent être revues, **cette position étant principalement motivée par le caractère sensible des données de santé**. La CNIL conseille par conséquent à HDH de recourir à une société non soumise aux lois américaines. **Jusqu'à ce qu'une solution alternative soit trouvée, la CNIL accepte qu'une période transitoire soit accordée** (non définie par la CNIL dans son mémoire en observations devant le Conseil d'Etat mais fixée ultérieurement, par courrier au ministère des Solidarités et de la Santé, à un délai compris entre 12 et 18 mois et, en tout état de cause, ne dépassant pas deux ans) **durant laquelle les transferts de données personnelles par HDH seront juridiquement fondés sur la dérogation de l'article 49-1 d) du RGPD** qui **autorise des dérogations aux exigences minimales de protection des transferts pour des motifs importants d'intérêt public,** reconnaissant que la Décision Schrems II entraîne juridiquement l'obligation de cesser un très grand nombre de transferts, ***ce qui peut dans certains cas, porter une atteinte disproportionnée à l'intérêt général***.

2.5. **Par l'ordonnance du 13 Octobre 2020**, le juge des référés du Conseil d'État observe que :

1) **les lois américaines de surveillance ne répondent pas aux Garanties Essentielles Européennes** (GEE) selon la Décision Schrems II,

2) HDH s'est engagé auprès de la CNIL à ce **qu'aucune donnée de santé ne soit transférée en dehors de l'UE**,

3) de plus, un **arrêté ministériel** en date du 9 octobre 2020 a été adopté par le ministère des Solidarités et de la Santé pour compléter l'article 30 de l'arrêté du 10 juillet 2020, **en vertu duquel aucune donnée personnelle ne pourra être transférée en dehors de l'UE** dans le cadre des traitements réalisés par HDH,

4) **HDH s'est contractuellement assuré que de telles exigences seront respectées par Microsoft**.

Le Conseil d'État relève ainsi que s'il existe un risque potentiel d'accès par les autorités américaines aux données personnelles traitées par HDH, dans l'hypothèse où Microsoft ne serait pas capable de s'y opposer, il existe **un intérêt public important à permettre le recours par HDH aux moyens techniques sans équivalent offerts par Microsoft pour poursuivre les traitements** aux fins de gérer l'urgence liée à la crise sanitaire. **Cet intérêt public peut également se justifier pour chaque projet** sous réserve que ce recours soit proportionné aux risques sanitaires encourus, à l'urgence s'attachant à sa conduite et à l'absence de solution technique alternative satisfaisante permettant d'y procéder dans les délais utiles. **Toutefois, en raison de la sensibilité particulière des données de santé, les autorités publiques ont fait part de leur volonté de réduire au maximum les risques que présente l'hébergement de données par un opérateur américain et de les faire disparaître complètement d'ici deux ans**. Dans l'intervalle, il est demandé à HDH d'obtenir de Microsoft des mesures techniques et organisationnelles supplémentaires pour garantir au mieux la protection des droits des personnes concernées et minimiser les risques.

3. Les raisons ayant conduit HDH à demander cette consultation

3.1. À la lumière du contexte décrit au paragraphe (2), HDH s'inquiète de l'approche très stricte de l'Autorité de Contrôle française (la "CNIL") et du Comité Européen de la Protection des Données (le « CEPD »)[3] exprimée dans ses recommandations émises à la suite de la Décision Schrems II, en particulier dans le cadre du scénario 6.

3.2. HDH a donc décidé d'évaluer les risques du choix de la solution offerte par Microsoft suite à la Décision Schrems II :

3.2.1. HDH souhaite une analyse pratique et objective (incluant une analyse de risques) **de la probabilité que les lois de surveillance américaines permettent aux autorités publiques américaines de contraindre Microsoft à leur donner accès aux données de santé traitées pour le compte du HDH sur ses serveurs au sein de l'UE**.

3.2.2. Depuis la Décision Schrems II, le champ d'application des lois américaines de surveillance fait l'objet d'interprétations diverses, voire d'une mauvaise interprétation nécessitant d'être clarifiée.

3.3. Les questions traitées ci-dessous ont pour objet d'apporter au HDH les clarifications demandées et d'identifier les arguments qui permettent de démontrer que le risque de transfert vers un pays tiers et d'accès non autorisé par des autorités publiques de ce pays, dénoncé par la CNIL est peu pertinent dans le contexte du traitement de

[3] Recommandations 01/2020 du Comité Européen de la Protection des Données (CEPD) du 10 novembre 2020

données personnelles par la plateforme HDH, où plusieurs mesures ont déjà été mises en œuvre avec Microsoft pour répondre aux problématiques soulevées par l'autorité de contrôle.

3.4. **Les réponses ci-dessous tiennent donc compte de la situation particulière de la plateforme HDH** et ne préjugent en rien d'autres situations où les risques soulevés par la CNIL et l'EDPB pourraient avoir leur pertinence.

4. Analyse Juridique

- ✔ **A titre préliminaire**, il conviendra de s'interroger sur **l'applicabilité de la Décision Schrems II au contexte de HDH**, étant donné la localisation des données du HDH en Europe et l'absence de tout transfert hors UE (4.1).
- ✔ Nous examinerons ensuite **l'applicabilité des lois de surveillance américaines visées par la Décision Schrems II** (4.2) et **celles non visées** par cette Décision, **à savoir le CLOUD Act** (4.2) au contexte de HDH.
- ✔ Quand bien même **la Décision Schrems II s'appliquerait**, nous verrons dans quelle mesure **HDH pourrait bénéficier de l'une des dérogations aux conditions de transfert prévues par l'article 49 du RGPD** (4.4)
- ✔ Nous verrons ensuite, à la lumière de ce qui précède **si des mesures techniques et organisationnelles supplémentaires s'avèrent nécessaires** pour la période de transition donnée à HDH **au regard des mesures en place et des risques soulevés** (4.5).
- ✔ Enfin, nous aborderons **les risques de violation de l'article 48 du RGPD que pourrait engendrer l'application des lois de surveillance** si Microsoft devait répondre aux requêtes des autorités sur leur seul fondement (4.6).

4.1. Sur l'inapplicabilité de la Décision Schrems II au contexte de HDH

L'examen de la Décision Schrems II et son interprétation par l'EDPB dans ses Recommandations 01/2020, notamment dans le cadre du scenario 6 (*couvrant le cas des transferts à des fournisseurs de services de cloud ayant besoin d'avoir un accès aux données en clair*), nous amènent à nous interroger sur son application au contexte du HDH pour les raisons suivantes :

4.1.1. **La Décision Schrems II ne couvre pas le scénario où une autorité d'un pays tiers aura accès aux données personnelles situées au sein de l'UE**, qui est pourtant le cas envisagé par la CNIL concernant le traitement des données par HDH qui restent sur un serveur en France.

DLA PIPER

4.1.2. Il est d'ailleurs intéressant de noter que le **Conseil d'État[4] confirme cette compréhension dans sa décision du 13 octobre 2020**, en ces termes « *il convient cependant de relever, en premier lieu, que la Cour de Justice s'est seulement prononcée, dans son arrêt du 16 juillet 2020, sur les conditions dans lesquelles peuvent avoir lieu des transferts de données à caractère personnel vers les Etats-Unis* ***et non sur celles dans lesquelles de telles données peuvent être traitées, sur le territoire de l'Union européenne****, par des sociétés de droit américain ou leurs filiales en qualité de sous-traitants voire de responsable de traitement* ».

4.1.3. En effet, le Conseil d'État, constate que **la CJUE ne s'est pas prononcée sur les conséquences que pourraient avoir sa décision sur des traitements effectués dans des circonstances semblables à celles de HDH**, tout en mentionnant la possibilité de se fonder sur les dérogations de l'article 49 du RGPD relatives au transfert de données personnelles vers des pays tiers, lorsque *ces transferts sont nécessaires pour des motifs importants d'intérêt public* reconnus par le droit de l'UE ou de l'État membre auquel le responsable de traitement est soumis.

4.1.4. **La Décision Schrems II intervient dans un contexte complètement différent** où des utilisateurs résidant au sein de l'UE (notamment M. Schrems) ont constaté que leurs **données personnelles étaient transférées par Facebook Ireland vers des serveurs appartenant à Facebook Inc.**, situés aux États-Unis. Un tel transfert était protégé, non seulement par la décision d'adéquation du Privacy Shield qui a été invalidée, mais aussi par les Clauses Contractuelles Types (CCT – responsable du traitement et sous-traitant) dont la CJUE a confirmé la validité.

4.1.5. **La Décision Schrems II a donc été rendue dans le contexte d'un transfert de données personnelles entre deux opérateurs économiques à des fins commerciales** (paragraphe 86) **dans le cadre de l'utilisation d'un réseau social ouvert au public**. C'est dans ces circonstances que le demandeur avait soulevé le risque que, malgré les CCT en vigueur, les données transférées puissent être accessibles par les autorités de surveillance américaines au moment du transfert ou après.

4.1.6. Ces circonstances factuelles expliquent que la CJUE, ait considéré **qu'un tel risque ne pouvait être exclu (notamment du fait de la nature du service en question, s'agissant d'un réseau social susceptible d'intéresser les autorités de surveillance dans le cadre de leur enquête**) dans la mesure où les réglementations américaines n'offraient pas de garanties suffisantes pour protéger les droits des personnes concernées. C'est ce constat qui l'a amené à conclure que lorsque les CCT ne peuvent suffire à garantir un niveau de protection équivalent à celui de l'UE, des mesures supplémentaires doivent être adoptées pour assurer la conformité avec le niveau de protection prévu par l'UE. A défaut, il faudra interrompre ou suspendre le transfert.

[4] Conseil d'État , Ordonnance du 13 octobre 2020, CNLL c/ HDH, paragraphe 18

4.1.7. **Appliquer la Décision Schrems II aux conditions de traitement des données par HDH, paraît excessif dans la mesure où dans le contexte de HDH, il n'y a pas de transfert de données puisque HDH, en conformité avec les différents avis de la CNIL, a obtenu de Microsoft que les données personnelles soient hébergées uniquement au sein de l'UE** (et même en France), **et que Microsoft Irlande et Microsoft US n'aient pas accès aux données hébergées sur leurs serveurs au sein de l'UE, y compris dans le cadre du support technique ou pour la résolution d'incidents**.

4.1.8. **Le seul cas de transfert envisageable** dans la situation actuelle du traitement effectué par HDH serait donc **celui où Microsoft devrait faire droit à une demande de communication adressée par les autorités américaines à Microsoft US**, malgré toutes les mesures techniques, organisationnelles et contractuelles en place.

4.1.9. Dans un tel cas qui nous paraît très théorique, **là encore la Décision Schrems II ne s'applique pas car le transfert qui interviendrait ne serait pas**, contrairement au transfert examiné dans la Décision Schrems II, **un transfert susceptible d'être couvert par les CCT**, dès lors qu'il ne s'agit pas d'un transfert de données effectué par HDH mais par Microsoft Irlande pour répondre aux demandes des autorités.

4.1.10. Dans une telle hypothèse, **le transfert résultant d'un accès fourni par Microsoft Irlande sur demande de Microsoft US** à la suite d'une injonction d'une autorité américaine, **rendrait Microsoft Irlande responsable du traitement** et non plus sous-traitant, la décision de transfert se faisant à l'initiative de Microsoft Irlande.

4.1.11. En effet, nous comprenons que selon la CNIL, le risque que Microsoft fournisse techniquement, un accès aux données personnelles traitées par HDH à une autorité américaine, ne peut être écarté dans la mesure où Microsoft Irlande ayant sa société mère aux Etats-Unis, est soumise au droit américain, et peut être enjointe de communiquer de telles données par l'intermédiaire de sa maison mère ou directement en tant que filiale d'une société américaine.

4.1.12. **Dans une telle hypothèse, Microsoft commettrait une violation grave du RGPD en tant que sous-traitant et manquerait à ses obligations au titre du contrat de service et des avenants signés avec HDH. Ce faisant, Microsoft devrait être considéré comme traitant les données personnelles** fournies par HDH **au-delà des instructions reçues**. En effet, Microsoft s'est engagé contractuellement à ne pas transférer de données de santé en dehors de l'UE, ni à accéder à ces données sans autorisation préalable du HDH.

4.1.13. Par conséquent, **Microsoft devrait être qualifié comme seul responsable du traitement résultant de ce transfert, conformément aux lignes directrices du CEPD** sur les notions de responsable du traitement et de sous-traitant dans le cadre du

RGPD[5] : « *Le sous-traitant ne doit traiter les données à caractère personnel que sur instruction du responsable du traitement [...] Un sous-traitant viole les dispositions du RGPD s'il outrepasse les instructions du responsable du traitement et commence à déterminer ses propres finalités et moyens du traitement. Le sous-traitant sera alors considéré comme un responsable du traitement dans le cadre de ce traitement et pourra s'exposer à des sanctions pour avoir outrepassé les instructions du responsable du traitement* ».

4.1.14. En donnant accès aux données personnelles du HDH sur ordre des autorités américaines sans l'autorisation de HDH, Microsoft répond à ses propres obligations légales ou à son intérêt légitime d'assurer sa défense mais ne suit aucune instruction donnée par HDH. Microsoft doit donc être considérée comme déterminant ses propres finalités et moyens du traitement. **Une telle qualification semble avoir également été envisagée par le Conseil d'État, dans sa décision du 13 octobre 2020, au considérant 18, où il retient que la Décision Schrems II ne couvre pas le cas où « *de telles données peuvent être traitées, sur le territoire de l'UE, par des sociétés de droit américain ou leurs filiales en qualité de sous-traitants, voire de responsables de traitement*. »**

4.1.15. A la lumière de nos développements précédents, il convient de conclure que **de nombreux arguments permettent de considérer que la Décision Schrems II n'est pas applicable à la situation du HDH**. De plus, au regard de toutes les mesures techniques, organisationnelles et contractuelles mises en œuvre par HDH, le seul transfert éventuel considéré par la CNIL comme présentant un risque pourrait ne pas être considéré comme un transfert sous la responsabilité du HDH en tant que responsable de traitement mais comme un transfert sous la responsabilité de Microsoft. **Par conséquent, HDH ne devrait pas être soumis aux règles spécifiques résultant de la Décision Schrems II**.

4.1.16. Si le risque de transfert vers les États-Unis ne peut être techniquement exclu, HDH se trouverait-il dans la situation du scénario 6 des recommandations 01/2020 du CEPD, en date du 10 novembre 2020, qui prévoient qu'aucune mesure supplémentaire ne peut être prise pour assurer une protection équivalente à celle existant au sein de l'UE, dès lors que « *le pouvoir accordé aux autorités publiques du pays destinataire d'accéder aux données transférées va au-delà de ce qui est nécessaire et proportionné dans une société démocratique* » ?

4.1.17. Cela est contestable dans la mesure où le *scénario 6 couvre le cas où un* ***« exportateur de données a recours à un fournisseur de services informatiques cloud ou à un autre sous-traitant pour le traitement de données à caractère personnel conformément à***

[5] Recommandations du CEPD sur les notions de responsable du traitement et de sous-traitant - 02 Septembre 2020

ses instructions dans un pays tiers»[6], ce qui implique une autorisation de l'exportateur de transférer les données. Or dans la situation du HDH, **HDH a clairement donné pour instruction à Microsoft de ne pas transférer les données, y compris aux fins des services de support technique et aucun transfert n'est effectuée vers un pays tiers. Le scénario 6 n'a donc pas vocation à s'appliquer à HDH.**

4.2. Sur l'inapplicabilité des lois de surveillance américaines visées par la Décision Schrems II au contexte de HDH

4.2.1. *Les services cloud de Microsoft Azure font partie des activités susceptibles d'être appréhendées par les lois de surveillance américaines*

Pour les définitions des termes en bleu, veuillez-vous reporter à l'Annexe 1 jointe au présent mémorandum.

a) **Dispositions de l'article 702 du FISA (Foreign Intelligence Surveillance Act) applicables aux prestataires de services cloud**

Pour faire l'objet d'une demande de renseignements au titre de l'article 702 du FISA, une entreprise doit correspondre à la définition de fournisseur de services de communications électroniques.

La définition des fournisseurs de services de communications électroniques inclut les « services informatiques à distance » (« *remote computing services* ») et les « services de communications électroniques » (« *electronic communications services* »), qui sont chacun définis comme des entités qui exercent des activités spécifiques liées aux « **communications électroniques** ».

Par conséquent, en tant que fournisseur d'un service d'informatique cloud, Microsoft est susceptible de relever de la définition d'un « fournisseur de services informatiques à distance », ce qui pourrait déclencher l'application de l'article 702 du FISA.

Lorsqu'on se réfère à l'article 702 de FISA, il existe deux programmes qui sont publics :

– **PRISM** (ou Downstream) et **UPSTREAM** – qu'il est important de comprendre. Ces programmes poursuivent des objectifs similaires mais visent des catégories différentes de fournisseurs de services de communications électroniques.

[6] Recommandations 01/2020 sur les mesures qui complètent les instruments de transferts destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE.

PRISM est un programme qui vise des fournisseurs de services internet américains tels que Microsoft qui ne constituent pas le « backbone » des réseaux de télécommunication.

UPSTREAM diffère en ce sens que la demande est envoyée aux entreprises américaines qui font partie des fournisseurs de réseaux / infrastructures des services de télécommunications.

Ainsi si l'article 702 du FISA devait s'appliquer à Microsoft, **ils seraient susceptibles d'être soumis plutôt au programme PRISM**, car Microsoft ne fournit pas de services généralement considérés comme des services d'infrastructures réseaux de télécommunications.

Dans le cadre de PRISM, l'Agence Nationale de Sécurité (NSA) doit identifier un mode de communication qu'il souhaite cibler (par ex : messagerie ou réseau social) et ensuite définir un identifiant unique (le « marqueur ») **qui sera associé à la personne/l'entité cible**. Cet identifiant unique n'est pas un mot clé (comme par exemple « nucléaire » ou « bombe ») **mais un véritable identifiant de communication, comme une adresse e-mail ou un numéro de téléphone**. La NSA se réfère à un marqueur « *à destination ou en provenance* », **c'est-à-dire qu'elle recherche des communications à destination ou en provenance de la personne liée au marqueur et donc d'une personne identifiée**. Il n'y a pas de liste prédéfinie de ces marqueurs.

Ces critères relatifs à la cible sont soumis à **une demande de surveillance autorisée en vertu de l'article 702 du FISA** et certifiés chaque année par le Procureur Général et le Directeur du Renseignement National. **Cette certification de la cible doit ensuite être approuvée par le tribunal FISA** (bien que les collectes de données en résultant n'aient pas à l'être). Le tribunal FISA va seulement vérifier si les critères nécessitant une surveillance de la cible sont vérifiés.

L'article 702 du FISA exige ainsi que les autorités américaines se conforment aux critères mentionnés ci-dessus lorsqu'elles procèdent à une surveillance autorisée, mais n'exige pas un examen individualisé de l'application de chaque programme de surveillance.

Une fois que la surveillance est approuvée selon les critères mentionnés ci-dessus, conformément aux exigences de la certification obtenue, elle est effectuée par les autorités publiques américaines qui fournissent à l'entreprise susceptible de détenir ces informations et basée aux États-Unis, ces marqueurs, tels qu'une adresse électronique ou un numéro de téléphone afin d'obtenir des informations sur une personne identifiée.

Dans le cadre de l'UPSTREAM, l'Agence Nationale de Sécurité (NSA) fournit des marqueurs du type « *à destination, en provenance ou à propos* », ce qui signifie qu'en outre, l'Agence Nationale de Sécurité peut collecter des **communications** « *à propos* » d'une cible envoyée par des personnes qui n'étaient pas la personne identifiée par les marqueurs, objet d'une demande de l'article 702.

***b)* Dispositions de l'EO12333 permettant son application aux prestataires de services cloud**

En ce qui concerne l'EO 12333, **les services d'hébergement de Microsoft pourraient être qualifiés de communications non publiques fournies par des moyens électroniques, lesquelles peuvent être soumises à une « surveillance électronique [7]»**, dans le cadre de l'EO 12333, seul terme utilisé par ce texte qui ne fait pas référence comme FISA à la notion de « communications électroniques ».

Ainsi, **si en théorie, l'activité de fournisseur de « services cloud » permet d'être appréhendée par les deux textes visés par la Décision Schrems II, les conditions de fond de leur application telles que développées ci-dessous ne sont pas vérifiées dans le cas des traitements du HDH**.

4.2.2. Les traitements effectués par HDH n'entrent pas dans le champ d'applications des lois de surveillance américaines

a) Article 702 du FISA

i. Critères d'application

➢ Champ d'application territorial

Le texte réglemente **la surveillance** des **communications de personnes non américaines** à des fins de renseignements étrangers.

S'il ne comporte pas de portée territoriale expresse applicable à l'emplacement des fournisseurs de services de communications électroniques auprès de qui des informations peuvent être exigées, le texte ne s'applique qu'à des entités relevant de la compétence des tribunaux américains.

L'article 702 de FISA ne réglemente pas et **ne donne donc pas aux autorités américaines l'autorisation d'effectuer une surveillance ciblée de personnes**

[7] EO 12333, Section 3.5(c).

étrangères auprès d'entreprises qui seraient situées en dehors des États-Unis et de la compétence des tribunaux de ce pays[8].

La question de savoir si une entreprise est soumise à la compétence des tribunaux américains est une question d'appréciation. Ainsi, les autorités publiques américaines pourraient mener leur enquête auprès d'entités situées aux Etats-Unis, ou cotées en bourse aux Etats-Unis, ce qui pourrait être le cas de Microsoft US mais cette dernière n'intervient pas dans le traitement des données qui restent en France. En revanche, il parait contestable que les autorités américaines puissent utiliser l'article 702 du FISA pour obtenir des données détenues par un fournisseur de services de communications électroniques, situé en France ou en Europe, dans la mesure où il ne relèverait pas de la compétence territoriale des tribunaux des Etats-Unis.

➢ Champ d'application matériel

Outre la nécessité de se situer dans le champ de compétence des tribunaux américains, deux autres critères s'appliquent : (1) la cible doit être une **puissance étrangère** ou un **agent d'une puissance étrangère** et (2) les marqueurs autorisés conformément à FISA 702 doivent pouvoir être utilisés.

Pour les définitions des termes **en bleu**, veuillez-vous reporter aux Annexes 1 & 2 jointes à la présente note.

(1) la cible de la surveillance en vertu de l'article 702 du FISA doit être une puissance étrangère[9]**, ou un agent d'une puissance étrangère**[10].

(2) La surveillance doit reposer sur des marqueurs autorisés

Comme nous l'avons vu précédemment au 4.2.1 (a) la surveillance envisagée d'une cible sur la base de marqueurs doit être conduite, conformément aux exigences de la certification obtenue du Procureur Général et du Directeur du Renseignement National **et être approuvée par le tribunal FISA.**

Ces marqueurs visant à obtenir des informations sur une personne identifiée sont un identifiant unique **qui est associé à la personne/l'entité cible**. Il s'agit d'**un véritable identifiant de communication, comme une adresse e-mail ou un numéro de téléphone (**marqueur « à destination ou en provenance »), dans la

[8] 50 U.S.C. § 1881a.

[9] Voir définition en langue ENG et FR en Annexe 1 et Annexe 2

[10] Voir définition en langue ENG et en Annexe 1 et Annexe 2

mesure où les recherches portent sur **des communications à destination ou en provenance de la personne liée au marqueur**.

ii. L'article 702 du FISA n'est pas applicable au contexte de HDH

A la lumière des conditions d'application de l'article 702 du FISA décrites ci-dessus, la mise en œuvre de l'article 702 du FISA pour tenter de contraindre Microsoft à fournir des données provenant de la plateforme HDH, n'est pas envisageable :

- **Le critère territorial n'est pas satisfait : la localisation des données et du fournisseur de services qui les héberge les placent probablement en dehors de la compétence des tribunaux américains puisque Microsoft Irlande est en Europe et non « basée aux US » et que les données ne sont pas hébergées par Microsoft aux US.** De même, HDH est un groupement d'intérêt public basé en France et ne peut donc être sollicité pour répondre à une telle demande.

- **Le critère matériel n'est pas non plus vérifié** :

  - HDH ne vérifie pas les critères de la cible requis par l'article 702 du FISA : **il ne répond pas à la définition de « puissance étrangère » ou « agent d'une puissance étrangère » et les types d'activités menées par le HDH n'entrent aucunement dans le champ d'application des activités mentionnées dans les définitions ci-dessus** (c'est-à-dire notamment les activités de terrorisme international, activités clandestines de renseignements, prolifération d'armes, etc.).

    De même, dans l'hypothèse où une personne dont les données sont présentes sur la plateforme de HDH, serait considérée comme « un agent d'une puissance étrangère », là encore l'article 702 du FISA ne pourrait s'appliquer dans la mesure où les données ne sont pas traitées dans le cadre « d'activités de terrorisme » mais à des fins de recherche dans le domaine de la santé.

  - Par ailleurs, nous comprenons que **les données sur la plateforme HDH sont des ensembles de données de santé pseudonymisées qui ne peuvent inclure, en principe, des communications par courrier électronique avec les marqueurs utilisés dans le cadre de l'article 702 de FISA, c'est-à-dire avec des personnes identifiées « à destination » ou « en provenance »**. Les marqueurs constituent des données directement identifiantes et non une combinaison de critères (ex : date d'hospitalisation, etc.). Par conséquent, **il n'est pas possible en pratique d'appliquer le programme PRISM au contexte de la plateforme HDH**, dans la mesure où **le recours aux marqueurs est inapplicable à des données**

pseudonymisées, et constitue un autre obstacle à l'utilisation de l'article 702 du FISA pour accéder aux données de la plateforme.

b) Executive Order 12333

i. Critères d'application

➢ *Champ d'application territorial*

Il est généralement admis que les activités de surveillance effectuées pour obtenir des informations de renseignements étrangers en dehors des États-Unis peuvent être effectivement autorisées par le président américain, de manière assez large.

À cet égard, l'EO 12333 permet la collecte d'informations de renseignements étrangers en dehors des États-Unis.

L'EO 12333 a été considéré par la CJUE comme pertinent dans la mesure où il est censé être utilisé pour intercepter les communications en transit vers les États-Unis (par exemple, en passant par des câbles Internet sous-marins), mais peut également s'appliquer aux données qui ne sont pas en transit.

➢ *Champ d'application matériel*

- **L'EO 12333 permet à une autorité publique américaine de collecter des données directement par ses propres moyens techniques**, mais ne peut servir de fondement juridique pour obliger une entreprise ou une entité qui les détient à lui fournir ces données.

  Par conséquent, même si une autorité américaine utilisait l'EO 12333 comme fondement pour demander à Microsoft ou HDH des données de la plateforme HDH, **l'EO 12333 ne contient pas de disposition qui obligerait HDH ou Microsoft à s'y conformer**.

- En outre, **l'objectif déclaré de l'EO 12333** est "***l'acquisition de renseignements étrangers importants, ainsi que la détection et la lutte contre les activités terroristes internationales, la prolifération des armes de destruction massive et l'espionnage mené par des puissances étrangères*** »).

ii. EO 12333 n'est pas applicable à la situation du HDH

➢ Le champ d'application territorial peut en théorie permettre l'utilisation de l'EO 12333

Comme l'EO 12333 permet à une autorité américaine d'exercer ses activités en dehors de l'UE, il n'y a théoriquement aucun obstacle qu'elle puisse l'exercer en France, à condition toutefois que cette activité de collecte des données soit effectuée directement par l'autorité concernée et par ses propres moyens.

Néanmoins, les critères du champ d'application matériel tels que décrits ci-dessous rendent l'EO 12333 inapplicable.

➢ le champ d'application matériel ne permet pas d'utiliser l'EO 12333 comme base juridique pertinente

- **Le mécanisme de l'EO 12333 est fondé sur un pouvoir accordé par le président des États-Unis à une autorité publique américaine pour qu'elle accomplisse sa mission d'investigation par ses propres moyens.**
  Par conséquent, si une autorité américaine recueille des informations au moyen des techniques autorisées par l'EO 12333, sur des serveurs situés en Europe, elle ne pourra le faire qu'à l'insu de HDH ou de Microsoft, par ses propres moyens d'investigation et de renseignement, car **l'EO 12333 ne lui permet pas de contraindre un tiers à lui fournir un tel accès, comme semble le penser la CNIL**.
- **Par ailleurs, la finalité de l'EO 12333** est d'obtenir des « *renseignements étrangers importants, ainsi que la détection et la lutte contre les activités terroristes internationales, la prolifération des armes de destruction massive et l'espionnage mené par des puissances étrangères* », ce qui **ne correspond nullement à la nature des données traitées par HDH (s'agissant de données de santé pseudonymisées collectées à des fins de recherche)** qui ne relèvent donc pas du champ d'application de l'EO 12333, et ne devraient donc pas faire l'objet d'une telle investigation.

Par conséquent, il est peu probable que les autorités américaines tentent d'utiliser l'EO 12333 pour obtenir des données stockées dans la plateforme HDH.

DLA PIPER

4.3. Bien que non mentionné par la Décision Schrems II, le CLOUD ACT (Clarifying Lawful Overseas Use of Data Act) est-il applicable à la situation du HDH ?

4.3.1. Critères d'application du CLOUD ACT

En 2018, les États-Unis ont promulgué la loi 'Clarifying Lawful Overseas Use of Data Act'[11] ("CLOUD Act"). Le CLOUD Act modifie le Stored Communications Act (« SCA »), qui fait partie de l'Electronic Communications Privacy Act (« ECPA »).

a) La localisation d'un prestataire relevant de la loi US

Le CLOUD Act s'applique en fonction de la localisation du prestataire de services, et non des données. Il offre ainsi aux autorités américaines la possibilité d'obliger Microsoft à fournir des données, quel que soit le lieu où se trouvent ces données. Ceci devrait donc être possible même si les données sont techniquement hébergées par Microsoft Irlande.

En effet, l'entité mère américaine qui est soumise au CLOUD ACT, est généralement considérée comme une entité de contrôle, capable de diriger les actions de ses filiales quelle que soit leur localisation dans le monde. Le gouvernement américain peut ainsi obtenir certaines données de communication même stockées à l'étranger dès lors que le fournisseur de services est basé aux États-Unis, même si ces données sont hébergées par les filiales hors des Etats-Unis.

L'application du CLOUD ACT permet un examen individualisé par les tribunaux américains (en vertu d'un mandat de perquisition d'un juge américain) des demandes de communication pour collecter des données de renseignement de manière autorisée par le CLOUD ACT. Le mandat de perquisition est accordé lorsqu'il y existe un « motif raisonnable » pour considérer que les informations à collecter constituent des preuves pour une enquête en cours.

b) Les autres critères

Pour être applicable, les conditions suivantes doivent être vérifiées de manière cumulative :

[11] Le CLOUD Act a été adopté dans le cadre de la H.R.1625 Consolidated Appropriations Act, 2018

- Pour permettre à une autorité américaine d'obtenir des données personnelles d'un fournisseur de services basé aux États-Unis ou de sa filiale située dans l'UE, **ces données doivent être en « possession, garde ou contrôle » (« *possession, custody or control*") du fournisseur de services sollicité**.

- **Les enquêtes menées en vertu du CLOUD ACT doivent porter sur des données relatives à des crimes relevant de la juridiction des États-Unis, par exemple un crime contre un ressortissant américain ou par un ressortissant américain**.

4.3.2. Le CLOUD ACT non plus n'est pas applicable à la situation du HDH

a) Le champ d'application territorial

L'application du CLOUD ACT suppose que Microsoft US puisse être en *« possession, garde ou contrôle »* des données stockées par Microsoft Irlande. Ce critère n'est pas vérifié dans le cadre du traitement effectué par HDH :

Du fait de leur chiffrement, les données stockées sur la plateforme du HDH au sein de l'UE, ne peuvent être en « *possession, garde ou contrôle* » de Microsoft US dans la mesure où ces données sont chiffrées par HDH avec ses propres clés qui sont elles-mêmes chiffrées et conservées dans le Module de Sécurité Matériel ("HSM") de Microsoft Azure Key Vault **et restent donc sous le contrôle de HDH**. Ainsi, même si les autorités américaines devaient utiliser le CLOUD ACT pour contraindre Microsoft US et Microsoft Irlande à fournir des données chiffrées par HDH, **celles-ci seraient inutilisables.**

Il s'agit d'une interprétation communément admise aux Etats-Unis, en l'absence de **jurisprudence.**

En tout état de cause, le deuxième critère d'application du CLOUD ACT n'est pas vérifié.

b) Le champ d'application matériel

Les données conservées sur la plateforme HDH étant des données de santé relatives à des individus en France, elles ne sont donc pas susceptibles d'entrer dans le champ d'application des informations qui seraient liées à la commission de crimes tels que visés par le CLOUD ACT. Ainsi même si une personne soupçonnée d'actes de terrorisme aux Etats-Unis se fait soigner en France et que ses données sont collectées de manière

pseudonymisée sur la plateforme technologique du HDH en relations avec son traitement médical, de telles données ne peuvent être soumises aux dispositions du CLOUD ACT car elles ne portent pas sur les actes de terrorisme qui lui sont reprochés (elles ne concernent que les soins fournis). Par ailleurs, comme le CLOUD ACT exige un examen individualisé du mandat de perquisition par des juges américains indépendants et un « motif raisonnable » pour collecter les renseignements autorisés par la loi nécessitant de démontrer que les preuves recherchées concernent une enquête criminelle en cours, une telle demande ciblant les données conservées sur la plateforme HDH ne pourrait donc aboutir devant les tribunaux américains car ne répondant pas à l'objectif visé par le texte. Le mandat doit être spécifique à la personne visée par l'enquête. En effet, un mandat demandant toutes les informations contenues sur la plateforme HDH ou un projet de recherche sans plus de précisions serait certainement considéré comme trop général.

4.3.3. *Lorsque les données sont chiffrées, les autorités américaines peuvent-elles accéder aux données du HDH lorsqu'elles sont temporairement déchiffrées pour leur utilisation par les porteurs des projets de recherche ? Existe-t-il une limite au pouvoir d'investigation des autorités dans le cadre des lois sur la surveillance ?*

Comme nous l'avons déjà indiqué plus haut, le seul fondement juridique qui permettrait à une autorité américaine d'accéder aux données déchiffrées sur les serveurs européens de Microsoft pourrait être le CLOUD ACT, du fait de son application extraterritoriale aux filiales de fournisseurs de services basés aux Etats-Unis.

Or comme nous l'avons démontré ci-dessus, il y a peu de chance qu'une demande de communication de données détenues par HDH soit considérée comme conforme aux exigences du CLOUD ACT. En effet, les autorités américaines ont besoin d'un mandat de perquisition d'un juge américain, qui n'est accordé que lorsqu'il existe un « motif raisonnable » et la démonstration que l'information recherchée constitue une preuve pertinente pour une enquête en cours qui doit être liée à des crimes américains.

Compte tenu de la nature des données traitées par le HDH, il n'est donc pas possible sur la base du CLOUD ACT **que les autorités américaines accèdent aux données de HDH,** même **lorsqu'elles sont temporairement déchiffrées pour les besoins de la recherche par les porteurs de projets, du fait de l'encadrement juridique très strict qui régit le mandat délivré pour mener une enquête sur la base du CLOUD ACT.**

En effet, la portée du mandat de perquisition délivré en vertu du CLOUD Act est limitée par l'exigence de « spécificité » du quatrième Amendement de la Constitution US. En vertu de cette exigence, le mandat doit décrire de manière spécifique l'information devant être collectée et ne peut être trop large ou général. En pratique le mandat doit donc porter sur une demande d'information spécifique à une personne identifiée

(comme un compte qu'elle détiendrait par exemple dans le cadre d'un service internet ou un ordinateur qui lui appartiendrait). Un mandat comportant une demande d'information sur toutes les données détenues par HDH, ou toutes les informations relatives à un projet de recherche, sans plus de précision, serait considéré trop large. Il est également important de noter que l'autorité publique américaine qui requiert le mandat devra démontrer que HDH est impliqué dans la commission d'un crime.

4.3.4. *Quelle est la probabilité que les autorités de surveillance américaines soient intéressées par les données de santé du HDH hébergées par Microsoft au sein de l'UE ? Si une telle probabilité existe, comment pourrait être justifiée une telle ingérence ?*

Il est très peu probable que les autorités de surveillance américaines aient un intérêt pour les données de santé traitées par HDH, pour les raisons explicitées ci-dessus.

Comme l'indique d'ailleurs le gouvernement américain dans un livre blanc publié en septembre 2020 (voir p. 2)[12], après la Décision Schrems II, la majeure partie des sociétés ne traitent pas de données intéressant les services de renseignement américains et ne recevront jamais de demandes de communication de données.

Même si Microsoft publie des rapports faisant état d'un certain nombre de requêtes qu'elle reçoit des autorités, ces requêtes concernent des comptes représentant une très petite portion de la base de clients de Microsoft. A titre d'exemple, Microsoft a fait état dans son rapport de juillet à décembre 2019 de 0-499 requêtes sur des contenus (les chiffres de Microsoft sont exprimés par tranche), sur 14,500-14,999 comptes.[13] Ces chiffres sont à rapprocher avec la communication de Microsoft en fin 2019, faisant état de 200 millions de comptes utilisateurs commerciaux actifs sur Office 365, ce qui ne représente que les utilisateurs d'un produit de Microsoft.[14]

Les rapports de Microsoft témoignent du peu de requêtes reçues par rapport au nombre de données traitées et de comptes utilisateurs concernés, confirmant le caractère très ciblé et circonscrit des lois de surveillance américaines et le fait que les demandes se rapportent à des comptes de services de communication électronique.

[12] US Government white paper September 2020

[13] See Microsoft U.S. National Security Orders Report

[14] See Microsoft Earnings FY20 Q1 Earnings Call Transcript

DLA PIPER

4.4. Si la décision Schrems II devait s'appliquer à HDH, comme le considère la CNIL, HDH peut-il bénéficier des exceptions de l'article 49 du RGPD ?

4.4.1. Dans sa décision (§202) du 16 juillet 2020, la CJUE affirme qu'« ***en tout état de cause, compte tenu de l'article 49 du RGPD, l'annulation d'une décision d'adéquation telle que la décision « Privacy Shield » n'est pas susceptible de créer un tel vide juridique*** ». En effet, cet article établit, de manière précise, les conditions dans lesquelles des transferts de données à caractère personnel vers des pays tiers peuvent avoir lieu en l'absence d'une décision d'adéquation en vertu de l'article 45, paragraphe 3, dudit règlement ou de garanties appropriées au titre de l'article 46 du même règlement.

4.4.2. Dans sa décision du 13 octobre 2020, le Conseil d'État reprend cette référence à l'article 49 du RGPD :

(§18) la Décision Schrems II « *ne s'est pas prononcée sur les conséquences que pourraient avoir les constats opérés par son arrêt [sur des traitements de données personnelles, tel que ceux effectués par des société de droit américains ou leurs filiales sur le territoire de l'UE], alors même que, s'agissant des transferts de données personnelles vers des pays tiers,* ***son arrêt en mentionne la possibilité sur le fondement de l'Article 49 du RGPD, qui permet les transferts nécessaires pour des motifs importants d'intérêt*** **public** ***reconnus par le droit de l'Union ou le droit de l'Etat membre auquel le responsable du traitement (ici, HDH) est soumis*** ».

(§20) "***il existe un intérêt public important à permettre la poursuite de l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le SARS-CoV-2 et, à cette fin, de permettre le recours aux moyens techniques, sans équivalent à ce jour, dont dispose la Plateforme des données de santé par le biais du contrat passé avec Microsoft*** ». **Même la CNIL dans son avis du 8 octobre 2020 se réfère (page 11) à cette dérogation de l'Article 49-1 (d) et plus précisément** à « *l'intérêt public manifeste à ménager cette période de transition, pour garantir la continuité de l'hébergement des données de santé et des usages qui y sont liés* ». La CNIL précise plus loin que « *maintenir temporairement le risque de ces transferts aux services de renseignements américains [...] s'avère provisoirement nécessaire pour garantir une transition satisfaisante vers un dispositif d'hébergement souverain des données de santé.* »

4.4.3. **Ce faisant, la CNIL et le Conseil d'Etat admettent la dérogation de l'article 49-1 d) mais de manière stricte** en justifiant son **application par la** situation spécifique couverte (recherche dans un contexte de crise sanitaire) qui satisfait ainsi le test de strict nécessité (urgence sanitaire). Ainsi le bénéfice de cette dérogation pour recourir à la solution Microsoft, nécessite que chaque projet de recherche soit examiné afin de s'assurer, pour chacun d'eux, si le transfert est justifié le temps de la période transitoire par « *les risques sanitaires encourus et appropriée aux circonstances de temps et de lieu, compte tenu, tout à la fois, de l'urgence s'attachant à sa conduite et de l'absence*

de solution technique alternative satisfaisante permettant d'y procéder dans les délais utiles ».

4.4.4. Les limites ainsi apportées (période transitoire, autorisation de transferts de manière limitée et sélective, etc.) au bénéfice du recours à la dérogation de l'article 49-1 d) appellent quelques interrogations : (i) le CEPD indique dans ses guidelines que la dérogation s'applique « *lorsqu'il peut être déduit du droit de l'Union ou du droit de l'Etat membre auquel le responsable de traitement est soumis que ces transferts de données sont autorisés pour des motifs importants d'intérêt public* », (ii) il semble donc que la CNIL et le Conseil d'Etat aient **déduit** des missions d'intérêt public du HDH reconnues par les textes de droit français (article L1462-1 du code de la santé publique et arrêté du 29 novembre 2019) que cette dérogation puisse servir de base légale du transfert dans la mesure où ces transferts ne sont pas explicitement visés par les textes ayant institué le HDH ; (iii) par conséquent on peut s'interroger sur les limites ainsi apportées par la CNIL et le Conseil d'Etat dans la mesure où les textes de référence n'opèrent pas de distinction entre les différents projets de recherche qui poursuivent tous une finalité d'intérêt public; (iv) l'article 49 du RGPD lui-même n'apporte pas de limites dès lors que les conditions de son application sont satisfaites . En effet, c'est lorsque le transfert ne peut être fondé sur aucun mécanisme de transfert (y compris les dérogations de l'article 49) qu'un encadrement strict, comme celui préconisé par la CNIL et le CEPD, doit être appliqué.

4.4.5. Par conséquent, **sur la base des décisions de la CJUE et du Conseil d'État ainsi que de l'avis de la CNIL, HDH est légalement fondé à utiliser la solution Microsoft même si elle présente à leurs yeux un risque potentiel de transfert des données personnelles aux États-Unis (en utilisant la dérogation d'intérêt public prévue à l'Article 49-I (d) du RGPD). Les limites apportées par la CNIL ne semblent pas véritablement fondées sur une base textuelle mais davantage sur son interprétation et celle du CEPD des dérogations de l'article 49, laquelle est discutable.**

4.4.6. Toutefois, **on peut s'interroger sur la compatibilité entre l'interdiction de transfert posée par l'arrêté ministériel du 9 octobre 2020 et la position prise par la CNIL et le Conseil d'État selon laquelle HDH peut continuer à utiliser de manière transitoire, la solution de Microsoft** avec un risque de transfert vers les Etats-Unis, **en se fondant sur la dérogation prévue par l'article 49 du RGPD.**

4.4.7. En effet, le recours à l'article 49 du RGPD laisse supposer un transfert à l'initiative du HDH. Or, comme nous l'avons vu précédemment, HDH a contractuellement obtenu de Microsoft qu'aucun transfert ne soit effectué même pour des raisons techniques. HDH est par ailleurs interdit d'autoriser tout transfert en vertu de l'arrêté susmentionné. Par conséquent si un risque de transfert vers les autorités de surveillance américaines devait exister, comme l'indique la CNIL, risque que le Conseil d'État considère comme

ne pouvant être exclu, un tel transfert ne peut être considéré comme étant à l'initiative du HDH mais seulement à celle de Microsoft pour les raisons développées précédemment aux sections 4.1.10 et suivantes.

4.4.8. Dans ces conditions, l'article 49 permettant le transfert des données pour des motifs d'intérêt public n'aurait pas lieu de s'appliquer à HDH. En effet, s'il y a un transfert vers les États-Unis, en raison des caractéristiques techniques de la solution Microsoft ou d'une demande des autorités américaines comme l'indique la CNIL, seul Microsoft serait à l'initiative d'un tel transfert sur une base légale qu'elle aura déterminée. Il lui appartiendra, en tant que responsable de traitement, de s'assurer que les données transférées seront protégées, étant entendu que ce transfert aura été effectué en violation de ses engagements contractuels avec HDH et à l'insu de HDH.

4.4.9. Ces transferts ne seraient de toute façon pas fondés dans la mesure où même les lois de surveillance américaines ne permettraient pas de les justifier.

4.4.10. A la lumière de ce qui précède, HDH pourrait tenter de demander à Microsoft, afin de témoigner des précautions supplémentaires demandées par le Conseil d'Etat et de rassurer la CNIL, **de lui garantir qu'aucun transfert ne sera effectué en vertu des lois de surveillance américaines mentionnées dans la Décision Schrems II, étant donné qu'il n'existe pas de motif juridique permettant aux autorités américaines de demander ces informations à Microsoft dans le contexte particulier du traitement de données de HDH**.

4.5. HDH est-il tenu de mettre en œuvre des mesures supplémentaires ?

La CNIL et le Conseil d'Etat prenant appui sur la Décision Schrems II et l'article 28 du RGPD, demandent à HDH de « *continuer à rechercher la mise en œuvre par Microsoft des mesures techniques et organisationnelles appropriées pour garantir au mieux la protection des droits des personnes concernées*. »

Cette requête résulte du risque de transfert vers les Etats-Unis considéré comme un pays ne présentant pas les Garanties Essentielles Européennes (GEE) (4.5.1) et nécessitant de ce fait que les CCT en place soient complétées par des mesures supplémentaires. Or, comme déjà développé précédemment, HDH n'étant pas à l'initiative de ce transfert, ces mesures supplémentaires n'ont pas lieu de lui être imposées et les conditions contractuelles, techniques et organisationnelles déjà mises en place dans le contexte de HDH permettent de démontrer que ces mesures supplémentaires ne devraient pas être nécessaires (4.5.2).

4.5.1. Les lois de surveillance américaines ne vérifient par les GEE

La décision Schrems II a considéré que les lois américaines de surveillance (Article 702 du FISA et EO 12333) ne vérifient pas les GEE définies dans ses Recommandations

DLA PIPER

02/2020 du CEPD du 10 novembre 2020[15] dans la mesure où elles se caractérisent par l'absence de :

a) règles claires, précises et accessibles (par exemple, champ d'investigation limité et précis, conditions spécifiques à respecter, etc.)

b) démonstration de la nécessité et de la proportionnalité du traitement au regard des objectifs légitimes poursuivis

c) mécanisme de surveillance indépendant

d) voies de recours effectives pour les personnes concernées

4.5.2. Néanmoins, HDH ne devrait pas être tenu de mettre en place des mesures supplémentaires

Même si les lois américaines de surveillance ne respectent pas les GEE, HDH a des raisons de considérer qu'il n'y a pas de nécessité de mettre en place des mesures supplémentaires :

a) **La Décision Schrems II ne s'applique pas au contexte de HDH.** Par conséquent les mesures supplémentaires qui en résultent ne peuvent être exigées.

b) **Dans la mesure où le risque de transfert dénoncé par la CNIL ne serait de toute façon pas à l'initiative de HDH,** il n'est donc pas pertinent de lui imposer de telles mesures supplémentaires, les CCT en place étant elles-mêmes sans objet puisqu'il n'y a pas de transfert possible par HDH ou sur ses instructions par Microsoft Irlande vers Microsoft US.

c) Enfin, la probabilité de l'application des lois de surveillance américaines n'étant pas vraisemblable comme indiqué plus haut, le risque que ce transfert ait lieu devrait être exclu, même si ce transfert était à l'initiative de Microsoft qui se mettrait en infraction au RGPD et violerait ses engagements contractuels en répondant à des autorités publiques.

Par conséquent les mesures déjà mises en place par HDH apparaissent appropriées pour garantir au mieux la protection des droits des personnes concernées, comme en témoignent les développements ci-dessous :

[15] Recommandations 02/2020 du CEPD du 10 Novembre 2020 sur les GEE

(1)Mesures contractuelles

Six avenants au Contrat avec Microsoft ont été signés par HDH afin de répondre aux inquiétudes de la CNIL et du Conseil d'État. Dans l'Avenant n°5 signé le 29 octobre 2020 à la suite de la décision du Conseil d'État, Microsoft a répondu à la demande du Conseil d'État en prenant les engagements suivants :

i. confirmation de l'application des lois de l'UE à Microsoft,
ii. mise en œuvre de processus internes pour répondre à toute demande de communication : engagement que Microsoft ne divulguera, ni ne donnera accès à une quelconque donnée traitée pour HDH aux autorités, sauf si la loi d'un Etat Membre l'exige. Microsoft s'engage à rediriger toute demande de communication de tiers à HDH à moins qu'il ne lui soit interdit de le faire et à contester cette demande en cas de conflit avec le droit de l'UE.
iii. localisation des données du HDH sur des serveurs situés dans l'UE. HDH a d'ailleurs obtenu un renforcement de cette garantie de localisation à travers un avenant n°6 signé le 6 avril 2021, lequel prévoit que « *Si le Client configure un service particulier à déployer dans une Zone, alors, dans le cadre de ce service, Microsoft entreposera et traitera les Données Client (y compris les Données à Caractère Personnel qui y sont incluses) dans la Zone spécifiée. Si le Client configure un service particulier en haute disponibilité/réplication dans une Zone répartie entre plusieurs Régions, alors, dans le cadre de ce service, Microsoft répliquera et traitera les Données Client (y compris les Données à Caractère Personnel qui y sont incluses) dans la Zone spécifiée, et les Régions composant cette Zone, uniquement* ». Par conséquent, aucune donnée de HDH n'est répliquée en dehors de la Zone France dans le cas de HDH.
iv. aucun accès n'est possible aux données du HDH même en vue d'une résolution des incidents grâce à la fonction de Lockbox
v. Microsoft conserve une copie « chiffrée » des clés de chiffrement utilisées par HDH pour chiffrer ses données au sein du Module de Sécurité Matériel (HSM) proposé par le service Azure Key Vault. Microsoft s'engage à ne pas tenter de contourner les procédures de chiffrement.

La description de toutes les mesures prises démontre que HDH a mis en œuvre la plupart des mesures contractuelles recommandées par le CEPD, en plus des mesures techniques et organisationnelles décrites ci-dessous.

Toutefois, **si HDH souhaitait compléter les mesures contractuelles existantes**, il pourrait éventuellement mettre en place les mesures suivantes :

- **signer la dernière version finalisée des CCT de la Commission Européenne dès qu'elles seront finalisées** et intégrer en particulier certaines stipulations spécifiques apportant plus de garantie (notamment celles mettant l'accent sur

la contestation des demandes d'accès des autorités et les mesures de renforcement spécifique des droits des personnes concernées).

- **Obtenir de Microsoft une garantie / confirmation expresse spécifique** au contexte du traitement des données par HDH **que les lois américaines de surveillance mentionnées dans la Décision Schrems II ne sont pas susceptibles de s'appliquer à HDH, de sorte que le risque de transfert soulevé par la CNIL n'est pas pertinent.**

(2)Mesures techniques

HDH ne traite que des données pseudonymisées. Ces données sont chiffrées par HDH avec ses propres solutions techniques.

Microsoft conserve une copie « chiffrée » des clés de chiffrement dans un équipement HSM qui permet l'utilisation des clés mais pas leur export. En outre, Microsoft s'engage expressément à ne pas tenter de contourner le chiffrement des données, y compris, mais sans s'y limiter, en essayant d'utiliser les clés stockées par HDH dans le service Azure Key Vault.

Les données sont stockées et traitées sur des infrastructures Microsoft Azure situées en France. Les différents services utilisés pour traiter et stocker les données sont certifiés pour l'hébergement des données de santé.

Ce faisant, HDH a mis en place l'ensemble des prescriptions indiquées par le CEPD dans sa réponse à la Question 12 de sa FAQ sur la Décision Schrems de la CJUE dans l'affaire C-311/18[16] :

En effet à la question : *que puis-je faire afin de continuer à utiliser les services de mon sous-traitant si le contrat signé en conformité avec l'article 28, paragraphe 3, du RGPD indique que les données peuvent être transférées vers les États-Unis ou un autre pays tiers ?*

Les réponses sont les suivantes :

- ✔ Si vos données peuvent être transférées vers les États-Unis et qu'aucune mesure supplémentaire ne peut être fournie pour s'assurer que le droit des États-Unis n'affecte pas le niveau de protection substantiellement équivalent, tel qu'il est garanti dans l'Espace Économique Européen (EEE) par les outils de transfert, les dérogations prévues à l'article 49 du RGPD ne

[16] FAQ sur l'arrêt rendu par la Cour de justice de l'Union Européenne dans l'affaire C-311/18 - Data Protection Commissionner contre Facebook Ireland Ltd et Maximilian Schrems

s'appliquent pas non plus ; ***la seule solution consiste à négocier une modification ou une clause supplémentaire à votre contrat pour interdire les transferts vers les États-Unis. Les données doivent être stockées, mais également administrées ailleurs qu'aux États-Unis***.

- ✔ Si vos données peuvent être transférées vers un autre pays tiers, vous devez également vérifier que la législation en vigueur dans ce pays tiers est conforme aux exigences de la Cour et au niveau de protection des données à caractère personnel escompté. Si aucun arrangement convenable n'est trouvé en matière de transfert vers un pays tiers, ***les données à caractère personnel ne doivent pas être transférées en dehors du territoire de l'EEE et toutes les activités de traitement doivent être réalisées dans l'EEE***.

HDH a ainsi obtenu de Microsoft que les données de santé soient conservées sur des serveurs situés en France et qu'aucune donnée ne soit transférée y compris aux fins de support technique. L'arrêté ministériel du 9 octobre 2020 confirme cette interdiction des transferts, qui doit être respectée par Microsoft.

Dans sa réponse, **le CEPD semble envisager la localisation des données offertes par des prestataires de service comme Microsoft, qui fournissent déjà leurs services à des sociétés européennes**, afin que celles-ci puissent restreindre les flux de données au sein de l'UE. **Le CEPD n'exige pas, comme le fait la CNIL, de choisir des prestataires de services soumis exclusivement au droit de l'UE**.

La FAQ du CEPD n'opère pas non plus de distinction entre données commerciales et **catégories particulières de données telles que les données de santé et préconise une localisation des données indépendamment de la catégorie des données concernées**.

En ce qui concerne **la gestion des données personnelles au sein de l'UE, nous comprenons que cette exigence est vérifiée** : Microsoft conserve une copie « chiffrée » des clés de chiffrement du HDH, dans le Module de Sécurité Matériel (HSM) de ses services Azure Key Vault et ces clés sont conservées au sein de l'UE sans possibilité d'export. Ces conditions sont contractuellement prévues par l'Avenant n°5 signé par HDH et Microsoft le 29 octobre 2020, à la suite de la décision du Conseil d'État, lequel prévoit que « *Lorsque le Client utilise le service Azure Key Vault pour stocker des clés de chiffrement et utilise ces clés pour chiffrer les Données Client stockées dans un Service en Ligne Microsoft, Microsoft ne tentera pas de contourner le chiffrement des Données Client y compris, mais sans s'y limiter, en essayant d'utiliser les clés stockées par le Client dans le service Azure Key Vault en l'absence d'instructions du Client à cet effet* ».

(3) Mesures organisationnelles

Microsoft ne peut pas accéder aux données situées sur la plateforme du HDH en clair sans manquer à ses obligations contractuelles.

Microsoft s'engage à ne pas divulguer, ni donner accès aux données aux autorités, sauf si la loi d'un État membre l'exige. Toute demande d'accès doit être fondée et justifiée par un ordre judiciaire et doit être valable et appropriée. Microsoft est connu pour avoir contesté plusieurs fois des demandes émanant des autorités devant les juridictions lorsque ces dernières étaient considérées par la société comme injustifiées, inappropriées ou en conflit avec ses obligations.

Microsoft publie un rapport semestriel sur la transparence comprenant un rapport sur les demandes formulées par les autorités judiciaires et un rapport spécifique sur les demandes formulées par les autorités américaines en rapport avec la sécurité nationale, comme le permet le droit applicable.

Toutes ces mesures sont en ligne avec les recommandations 01/2020 du CEPD et permettent de s'assurer que toutes les mesures disponibles ont été prises pour garantir la minimisation des données et les restrictions d'accès aux autorités non autorisées.

4.5.3. *Enfin, l'exigence de mesures supplémentaires par la CNIL et le Conseil d'État est contestable pour les raisons suivantes :*

- **Elle n'est pas conforme à la Décision Schrems II, laquelle exige de mettre en œuvre des mesures supplémentaires à la suite d'une analyse au cas par cas, après avoir évalué que le mécanisme de transfert en place n'assure pas une protection adéquate,** ce qui n'est pas le cas en l'espèce puisque le champ d'application des lois de surveillance, tout comme la nature des données traitées par HDH qui ne sont pas dans la finalité des enquêtes régies par les lois de surveillance, rendent improbable l'accès aux données (indépendamment de la personne concernée) et ne devrait donc pas affecter la protection garantie par les CCT en place.
- **Elle n'est pas conforme à l'approche du RGPD fondée sur l'analyse des risques (Considérant 74)** laquelle exige que le responsable du traitement mette en œuvre des mesures effectives et que ces mesures « *devraient tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que du risque que celui-ci représente pour les droits et libertés des personnes physiques.* » À la lumière de notre analyse ci-dessus, un tel risque étant ici limité, voire exclu, des mesures supplémentaires ne semblent pas nécessaires.

DLA PIPER

4.6. Si les lois de surveillance américaines sont susceptibles de s'appliquer à Microsoft, comme l'indique la CNIL, l'article 48 du RGPD ne constitue-t-il pas un obstacle à la communication de données personnelles aux autorités de surveillance américaines ?

4.6.1. Conformément à l'article 48 du RGPD, une demande de communication de l'autorité de surveillance américaine ne constitue pas un fondement juridique suffisant pour contraindre une société établie dans l'UE à fournir les informations demandées.

L'article 48 dispose que : « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ».

Le CEPD[17] a d'ailleurs confirmé que l'article 48 du RGPD vise à garantir que lorsqu'un jugement ou une décision d'une autorité administrative d'un pays tiers oblige un responsable du traitement ou un sous-traitant établi dans l'UE à divulguer des données personnelles, cette obligation doit être fondée sur un accord international pour être exécutoire dans l'UE.

Ainsi, une décision ou un jugement ou une ordonnance de production d'une autorité d'un pays tiers n'est pas suffisant pour justifier et rendre licite la communication de données personnelles. Plus précisément, « *une demande d'une autorité étrangère ne constitue pas en soi un motif légal de transfert* ». La décision ne peut être reconnue que « *si elle est fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers requérant et l'Union ou un État membre* »[18].

Par conséquent, Microsoft Irlande ne peut valablement communiquer des données personnelles aux États-Unis sur la base d'une ordonnance d'injonction des autorités américaines si cette demande n'est pas fondée sur un accord international entre l'Etat Membre (ici, la France) ou l'UE et les États-Unis. Elle se mettrait en infraction avec l'article 48 du RGPD qu'elle est tenue de respecter (étant un sous-traitant établi en Europe) et violerait ses obligations contractuelles à l'égard de HDH.

[17] EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (Comité Européen de la Protection des Données – Contrôleur Européen de la Protection des Données Réponse conjointe à la Commission des Libertés Civiles, de la Justice et des Affaires Intérieures sur l'impact du Cloud Act sur le cadre légal européen applicable à la protection des données personnelles

[18] Annex of the EDPB-EDPS Joint Response (Annexe de la réponse conjointe)

Cette interprétation a été confirmée par le Contrôleur Européen de la Protection des Données et le CEPD qui ont confirmé, que « *l'article 48 indique clairement qu'une décision de justice étrangère ne rend pas, en tant que telle, un transfert licite en vertu du RGPD* »[19].

La formulation de l'article 48 du RGPD est d'ailleurs assez large pour englober une demande de communication adressée non seulement à un responsable de traitement ou à un sous-traitant établi dans l'UE, mais également à un responsable de traitement ou à un sous-traitant établi aux États-Unis, mais soumis au RGPD en raison de sa portée extraterritoriale.

Si l'article 48 ne peut pas s'appliquer, d'autres mécanismes de transfert existent en vertu du chapitre V du RGPD dans le cas d'un transfert de données entre deux responsables du traitement aux fins de communication ultérieure à une autorité américaine par le destinataire, telle que l'une des dérogations prévues à l'article 49. Microsoft ne peut toutefois utiliser dans son cas une telle dérogation car un tel transfert ne serait soumis à aucune des garanties prévues par le RGPD, comme l'exige l'article 44, ce qui exposerait Microsoft à un risque de violer ses obligations contractuelles avec HDH et le RGPD.

Par conséquent, tout transfert de Microsoft sur demande d'une autorité de surveillance américaine violerait les dispositions de l'article 48 du RGPD et tout transfert pour des raisons techniques violerait les dispositions du contrat conclu avec HDH. Il semble donc peu probable que Microsoft prenne l'initiative d'un tel transfert à l'insu de HDH.

[19] Brief of the European Commission on behalf of the European union as Amicus Curiae un support of neither party, December

DLA PIPER

ANNEXE 1 : QUELQUES DEFINITIONS

En Anglais

1. *"electronic communication " under section 702 du FISA and EO 12333*

a) FISA

A request for information under Section 702 FISA may be made to '***electronic communications services providers***', which are defined as follows:

(i) A telecommunications carrier, as that term is defined in Section 153 of Title 47.
(ii) A provider of electronic communication service, as that term is defined in Section 2510 of Title 18.
(iii) A provider of a remote computing service, as that term is defined in Section 2711 of Title 18.
(iv) Any other communication service provider that has access to wire or electronic communications either as such communications are transmitted or stored.
(v) An officer, employee or agent of an entity described in subparagraphs (i), (ii), (iii) or (iv) above.

The terms '***electronic communication service***' and '***remote computing service***' are defined by reference to the ECPA, as follows:

- '*Electronic communications service*' means any service which provides to users thereof the ability to send or receive wire or electronic communications.
- '*Remote computing service*' means the provision to the public of computer storage or processing services by mean of an 'electronic communications system'.
- '*Electronic communications system*' means any wire, radio, electromagnetic, photo optical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.
- "*Electronic communication*" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce, but does not include:
  (A) any wire or oral communication;
  (B) any communication made through a tone-only paging device;
  (C) any communication from a tracking device; or
  (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

b) EO 12333

EO 12333 does not define the term 'electronic communication'. It does use the term 'electronic surveillance[20]', *which means the acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.*

EO 12333 delegates to the US Attorney General the authority in certain cases to authorize electronic surveillance, which may be conducted in accordance with FISA.

2. *Foreign Power and Agent of Foreign Power under FISA:*

a) Under FISA "foreign power"[21] means:

A. A foreign government or any component thereof, whether or not recognized by the US;
B. A faction of a foreign nation or nations, not substantially composed of US persons;
C. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
D. A group engaged in international terrorism or activities in preparation therefor;
E. A foreign-based political organization, not substantially composed of US persons;
F. An entity that is directed and controlled by a foreign government or governments; or
G. An entity not substantially composed of US persons that is engaged in the international proliferation of weapons of mass destruction.

b) There are two definitions in FISA for 'agent of a foreign power'[22]
One that applies to **non-US persons** and one that applies to all persons, including **US persons**. It is important to note that the first definition, which

[20] EO 12333, Section 3.5(c).

[21] 50 USC § 1801(a).

[22] 50 USC § 1801(b).

applies only to non-US persons, is broader and less tied to criminal violations of US law.

(i) **With respect to non-US persons**, '*agent of a foreign power*' is defined as a person who:

A. *Acts in the US as an officer or employee of a foreign power* or a member of a foreign power, irrespective of whether the person is inside the US.

B. *Acts for or on behalf of a foreign power that engages in clandestine intelligence activities in the US contrary to the interests of the US*, when the circumstances indicate that such person may engage in such activities or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities.

C. *Engages in international terrorism or activities in preparation* therefore.

D. *Engages in the international proliferation of weapons of mass destruction or activities* in preparation therefore.

E. *Engages in the international proliferation of weapons of mass destruction or activities in preparation therefore for or on behalf of a foreign power*, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefore.

(ii) **For all persons, including US persons**, 'agent of a foreign power' is defined to mean a person who:

A. *Knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power*, which activities involve or may involve a violation of the criminal statutes of the US.

B. *Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power*, which activities involve or are about to involve a violation of the criminal statutes of the US.

C. *Knowingly engages in sabotage or international terrorism or activities* that are in preparation therefore for or on behalf of a foreign power.

D. *Knowingly enters the US under a false or fraudulent identity for or on behalf of a foreign power* or, while in the US, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power.

E. *Knowingly aids or abets any person in the conduct of activities described in* Subparagraph (A), (B) or (C) or knowingly conspires with any person to engage in activities described in Subparagraph (A), (B), or (C).

DLA PIPER

ANNEXE 2 : QUELQUES DEFINITIONS

En Français

- Selon le FISA "**puissance étrangère**" ('foreign power')[23] signifie :

  A. Un gouvernement étranger ou toute composante de celui-ci, qu'il soit ou non reconnu par les États-Unis ;
  B. Une faction d'une ou plusieurs nations étrangères, non composée en majeure partie de ressortissants américains ;
  C. Une entité ouvertement reconnue par un ou plusieurs gouvernements étrangers comme étant dirigée et contrôlée par ce ou ces gouvernements étrangers ;
  D. Un groupe engagé dans le terrorisme international ou dans des activités préparatoires au terrorisme ;
  E. Une organisation politique basée à l'étranger, qui n'est pas majoritairement composée de ressortissants américains ;
  F. Une entité qui est dirigée et contrôlée par un ou plusieurs gouvernements étrangers ; ou
  G. Une entité non majoritairement composée de ressortissants américains et engagée dans la prolifération internationale des armes de destruction massive.

- S'agissant d'un 'agent d'une puissance étrangère' ('agent of a foreign power')[24], il y a deux définitions dans le FISA : l'une s'appliquant aux personnes non américaines et l'autre s'appliquant à toutes les personnes, y compris les personnes américaines. Il est important de noter que la première définition, qui s'applique uniquement aux personnes non américaines, est plus large et moins liée aux violations pénales du droit américain.

  En ce qui concerne les personnes non américaines, '**agent d'une puissance étrangère**' vise une personne qui :

  A. Agit aux Etats-Unis en tant que dirigeant ou employé d'une puissance étrangère ou membre d'une puissance étrangère, que la personne se trouve ou non aux Etats-Unis.
  B. Agit au nom ou pour le compte d'une puissance étrangère qui se livre à des activités clandestines de renseignement aux États-Unis contraires aux intérêts des États-Unis, lorsque les circonstances indiquent que cette personne peut se livrer à de telles activités ou lorsque cette personne aide ou encourage sciemment toute personne à se livrer à de

[23] 50 USC § 1801(a). Voir la version originale du texte en Annexe 1

[24] 50 USC § 1801(b). Voir la version originale du texte en Annexe 1

telles activités ou conspire sciemment avec toute personne pour se livrer à de telles activités.

C. Se livre à des activités de terrorisme international ou à des activités préparatoires à cette fin.
D. Se livre à la prolifération internationale d'armes de destruction massive ou à des activités préparatoires à cette fin.
E. Se livre à la prolifération internationale d'armes de destruction massive ou à des activités préparatoires en vue de cette prolifération pour le compte d'une puissance étrangère, ou aide ou soutient en connaissance de cause toute personne se livrant à cette prolifération ou à des activités préparatoires en vue de cette prolifération, ou conspire sciemment avec toute personne pour se livrer à cette prolifération ou à des activités préparatoires en vue de cette prolifération.

En ce qui concerne toutes les personnes, y compris les américains, **'agent d'une puissance étrangère'**, vise une personne qui :

A. S'engage sciemment dans des activités clandestines de collecte de renseignements pour ou au nom d'une puissance étrangère, activités qui impliquent ou peuvent impliquer une violation des lois pénales des Etats-Unis.
B. Se livre sciemment à d'autres activités clandestines de renseignement, conformément aux instructions d'un service ou d'un réseau de renseignement d'une puissance étrangère, pour ou au nom de cette puissance étrangère, qui impliquent ou sont en passe d'impliquer une violation des lois pénales des États-Unis.
C. Se livre sciemment à des actes de sabotage ou de terrorisme international ou à la préparation de tels actes pour le compte ou au nom d'une puissance étrangère ou en son nom.
D. Entre sciemment aux États-Unis sous une identité fausse ou frauduleuse pour le compte ou au nom d'une puissance étrangère, ou, pendant son séjour aux États-Unis, prend sciemment une identité fausse ou frauduleuse pour le compte ou au nom d'une puissance étrangère.
E. E. Aide ou assiste sciemment une personne dans la conduite des activités décrites aux sous-paragraphes A, B ou C ou conspire sciemment avec une personne pour se livrer aux activités décrites aux sous-paragraphes A, B ou C.

Avis de la Direction interministérielle du numérique (DINUM) sur le projet de Health Data Hub

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Direction interministérielle du numérique

Le directeur

Paris, le 10/11/2020

A Madame Stéphanie Combes, directrice générale du GIP Plateforme de données de santé

Objet : **Avis sur le projet Health Data Hub**

Réf : - Courrier de saisine du 09 octobre 2020
- Annexe : services utilisés par la plateforme

Conformément au contrat de transformation du fonds pour la transformation de l'action publique (FTAP), vous m'avez saisi par courrier du 09 octobre 2020 pour avis concernant le projet « Health Data Hub » (HDH).

Je remercie tout d'abord le groupement d'intérêt public (GIP) pour la collaboration tant dans la préparation de ce dossier que dans son déroulement, dans un contexte de crise COVID d'une part et une période particulièrement chargée pour vous-même et vos équipes d'autre part.

Le projet HDH vise à mettre à disposition des environnements sécurisés où pourront être réalisés des projets d'intérêt public sur des données de santé pseudonymisées provenant de sources multiples. La plateforme HDH, nationale et centralisée, permet la réalisation des projets de recherche dans des conditions de sécurité et de traçabilité inégalées et sur un périmètre de données ciblées pour des utilisateurs habilités.

Si la crise sanitaire a freiné la mise en œuvre de la plateforme, des projets liés au COVID délivrent déjà leur valeur, notamment au travers de l'exploitation des données des bases OSCOUR de Santé Publique France, SNDS Fast Track de la CNAM ou encore SIVIC de la DGS, dont les réutilisateurs sont principalement publics (DREES, INSEE, université de Grenoble) avec une mise en place en cours pour la société privée Clinityx.

Le succès de la plateforme se traduit par les nombreuses (plus de 250) candidatures des deux appels à projets en janvier et décembre 2019. Le processus de sélection des projets a permis d'en retenir 36 dont la mise en œuvre s'étale sur l'année 2021. Plusieurs ouvertures

Réf : CMR-2020-048
Affaire suivie par Pierre Casciola (département PSN)
Tél : 01 85 58 11 59- Mél : pierre.casciola@modernisation.gouv.fr
20, avenue de Ségur - 75007 PARIS

de projet sont prévues d'ici la fin du premier trimestre 2021, dont les réutilisateurs sont multiples (ICANS, EHESP, APHP, INSERM, Institut Curie, Centre Léon Berard de Lyon, CHU Limoges, DRCDC Occitanie, ARS IDF, CHU Bordeaux), avec également quelques structures privées (Implicity, E-Scopics ou encore l'ESPIC Fondation A. de Rothschild).

Vous avez pris soin de mandater un comité indépendant d'experts pour juger de la pertinence, de l'intérêt général, de l'adéquation des données demandées et de la méthodologie proposée de chacun des projets dans le cadre du processus de sélection. La valeur recherchée par ces projets n'est donc pas à discuter dans le cadre de la présente procédure. De plus, je considère que ces projets pris dans leur ensemble n'auraient pu se faire en dehors d'une telle plateforme au regard de la quantité de données à traiter et de la multiplicité des sources à manipuler dans les conditions de sécurité, de traçabilité et de délai nécessaires ne pouvant être atteintes par les projets individuellement.

Si l'ensemble des fonctionnalités de la plateforme prévues dans le dossier FTAP n'est pas encore complètement en place, je note que vous proposez un accompagnement personnalisé des projets à la fois pour l'appropriation des outils à disposition mais aussi pour permettre leur évolution en fonction des besoins projet. Par ailleurs, un comité scientifique et médical est en charge de recommander les prochains logiciels à installer sur la plateforme. Je note également la présence d'un Groupe de Travail sur les Logiciels visant à 1) recommander des logiciels à installer sur la plateforme du HDH, 2) proposer un « pipeline de certification » pour l'éligibilité des logiciels disponibles à la demande sur la plateforme, et 3) encourager le développement de logiciels et codes de recherche réutilisables pour permettre leur mise à disposition aux autres utilisateurs du HDH. Ces actions sont de nature à me rassurer concernant le bon déroulement des projets vis-à-vis de la valeur recherchée et d'une bonne gouvernance entre les outils utilisés et les développements faits dans le cadre des projets de recherche.

Après étude du dossier et des informations complémentaires échangées pendant la période d'instruction, je souhaite partager avec vous les points d'attention suivants nécessitant des mesures correctives et d'amélioration continue :

1. L'architecture en place est de qualité et à l'état de l'art, mais des éléments non redondés mettent en évidence l'existence de SPOF (single point of failure : points de défaillance uniques). Si des exigences de disponibilité réduites au lancement de la plateforme sont compréhensibles dans le cadre de projets de recherche scientifique et assumées par l'équipe du GIP, le délai de restauration / reconstruction de ces SPOF doit être améliorée.

   La réplication des données sur 3 sites de région parisienne est de nature à accélérer la remise en service de la plateforme en cas d'incident grave sur le datacenter principal hébergeant les services nécessaires à son fonctionnement.

   La plateforme répond aux exigences de sécurité de l'ANSSI, ce qui a permis ses homologations successives, dont la dernière a été prononcée le 28/10/2020 pour une durée de trois ans.

2. La réversibilité de la plateforme, bien que théoriquement évoquée dans les contrats des marchés support, doit faire l'objet d'une attention renforcée pour qu'elle puisse se dérouler dans des conditions financières et calendaires acceptables. L'étude de

réversibilité fournie est incomplète et ne permet pas d'établir un plan d'actions clair de nature à rassurer sur la capacité du HDH à être transféré vers un autre acteur du cloud offrant un panel de services similaires. Je note que la réversibilité est une préoccupation majeure du GIP, qu'une analyse complémentaire est en cours avec mes équipes, et que le GIP s'engage à mettre à jour cette étude annuellement.

3. Aucun processus d'optimisation des coûts permis par les infrastructures cloud n'a encore été mis en place. Sur les 11 M€ de coûts de fonctionnement annuels, 8,3 M€ sont provisionnés pour les projets (à date au nombre de 36 sur 2021) et 2 M€ pour le cœur de la plateforme (dont 400 k€ sur la volumétrie des données). Ces coûts sont cohérents et au niveau du marché pour un tel usage. Ils demandent toutefois à être optimisés conformément aux bonnes pratiques de consommation de services de cloud public.

   Les coûts annuels de personnel (1,2 M€ T2) nécessaires à l'exploitation, MCO et MCS de la plateforme, appuyés par un recours aux renforts externes (en diminution de 36% à compter de 2023 pour se stabiliser à 1 M€) sont en ligne avec la maturité du projet.

4. Les engagements pris envers les citoyens sont un engagement fort du GIP visant à assurer de la transparence sur la plateforme et son usage : intérêt général, protection des données, respect des droits individuels, mais également informations sur les projets de recherche en cours ou à venir. Si la liste des projets est présente sur le site www.health-data-hub.fr, les informations disponibles sur les projets mériteraient d'être détaillées, afin que les réutilisateurs fassent eux aussi preuve de transparence concernant les projets qu'ils mènent en s'appuyant sur les données mises à leur disposition par la collectivité.

Au vu de ces éléments, les mesures suivantes devraient être mises en place dans les plus brefs délais, compte tenu de la croissance du nombre de projets que vous attendez pour les mois à venir :

1. Un plan de reprise d'activité (PRA) de la plateforme doit être réalisé et documenté, avec en plus de l'externalisation des sauvegardes, la préparation de matériels de rechange, et un travail d'architecture de résorption des SPOF.
2. En termes de sécurité, l'ANSSI souligne le travail important réalisé par le GIP pour améliorer la sécurité de ses plateformes, en particulier sur le stockage des tables de correspondances par opérateurs. En plus de maintenir l'analyse de risque à jour au regard des évolutions techniques et fonctionnelles apportées à la plateforme HDH, l'ANSSI suggère d'améliorer en continu la détection et la réponse à incident : de nombreux indicateurs ont été mis en place, mais le GIP doit améliorer la capacité de ses équipes de supervision à détecter et traiter les événements de sécurité.
3. Le plan de réversibilité doit être finalisé et tenu à jour : Une première analyse des services utilisés par la plateforme est fournie en annexe du présent avis mettant en lumière un premier niveau d'effort pour permettre l'intégration de chacun des services nécessaires au HDH. Cette étude devra être poursuivie et partagée dans l'établissement d'un cahier des charges en chiffrant le coût et la durée de substitution / transfert des services en fonction des cas d'usage, des exigences de performance et du niveau de criticité pour le HDH (fonctionnalité indispensable, fonctionnalité dont

l'étude d'une alternative peut être considérée, ou fonctionnalité de confort). Tout nouvel usage de services Azure Cloud non utilisés pour la version 1 devra être conditionné à son niveau de réversibilité et à la non remise en cause du cahier des charges des futurs services Cloud qui aura été établi.

Je tiens à préciser que l'analyse réalisée par nos équipes dans le cadre de cette procédure est de nature à me rassurer sur le fait que les choix réalisés à date par le GIP n'obèrent pas la transférabilité de la plateforme, moyennant des efforts de reconfiguration et redéveloppement de certains composants précisés en annexe. Entre autres, aucun service d'intelligence artificielle d'azure n'est utilisé sur la plateforme. Je vous demande de maintenir à jour cette l'étude de réversibilité en continuant l'analyse par service dans le but de capitaliser sur les investissements déjà réalisés, et d'évaluer la réintégration de certains services au gré de l'augmentation de leur utilisation. Mes équipes se tiennent à votre disposition dans ce cadre.

4. La mise en place d'une démarche d'optimisation des coûts d'usage cloud (« FinOps ») doit permettre de limiter les coûts de fonctionnement (achat de services) de la plateforme cloud au juste nécessaire. Cette optimisation permettra de réinvestir les budgets provisionnés pour les projets (et non dépensés) sur l'évolution de la plateforme et l'absorption de nouveaux projets.
5. Concernant les coûts de personnel, les activités de chaque grande catégorie de service offert (collecte de données, distribution de données, sécurité, création de plateforme projet) doivent faire l'objet de procédures écrites permettant d'en envisager leur automatisation selon des critères de sensibilité, de répétition, etc. Ces automatisations, lorsque pertinentes, permettront de gagner en fiabilité et en coût de personnel. Le plan de recrutement du GIP devra également tenir compte de la montée en charge.
6. Une présentation des projets sous l'angle du bénéfice (avéré ou recherché) avec une documentation claire et accessible par les citoyens mériterait d'être mise en place. Au-delà de l'aspect positif d'une telle communication sur la population, elle sera également un vecteur complémentaire d'attractivité des réutilisateurs privés.

Au vu des efforts engagés par le HDH pour conduire ce programme et de l'attente forte de l'écosystème de la recherche médicale, je considère que les éléments précités ne sont pas d'ordre à le remettre en cause. Afin de conserver et renforcer la dynamique engagée depuis le début du projet, **j'émets un avis favorable sur le projet « HDH » sous réserve de la prise en compte des recommandations précédentes.**

Je souhaite à ce titre être informé de l'avancement des travaux et de l'application effective des recommandations.

Nadi BOU HANNA
Directeur interministériel du Numérique

_____

Copie :

Etienne CHAMPION

Secrétaire Général des ministères chargés des affaires sociales

Fabrice LENGLART

Directeur de la recherche, des études, de l'évaluation et des statistiques

Hélène BRISSET

Directrice du numérique

Laura LETOURNEAU

Déléguée ministérielle au numérique en santé

Livre blanc de Yes We Hack

LIVRE BLANC

DIVULGATION COORDONNÉE DE VULNÉRABILITÉS

FÉDÉRER POUR RÉDUIRE LE RISQUE

YES WE HACK

LIVRE BLANC

DIVULGATION COORDONNÉE DE VULNÉRABILITÉS

FÉDÉRER POUR RÉDUIRE LE RISQUE

YES WE HACK

/ SOMMAIRE

INTRODUCTION

L'essor du numérique et de l'innovation technologique est devenu le vecteur de bouleversements dans tous les aspects de notre vie. Les impacts de cette révolution numérique ont des répercussions sur tous les secteurs d'activité.
Nos vies connectées sont façonnées par ces innovations numériques, avec la négociation permanente entre confort d'usage et risque d'impact si quelque service dysfonctionnait.

La sécurité des innovations numériques est ainsi concernée au premier chef par ce bouleversement. La fluidité de l'information et la facilité des accès à distance font bouger les lignes du rapport individu-espace-temps. De nouvelles manières d'éprouver la sécurité et la qualité des services numériques apparaissent et s'imposent, induisant de nouvelles possibilités d'organisation de la sécurité. Les collaborateurs d'une entreprise, les membres d'une famille ou les amis souhaitant organiser une fête, évoluent graduellement vers une dématérialisation des échanges d'informations dans tous les domaines d'activité.

Ce qui semblait immuable apparaît aujourd'hui comme presque volatil. Ce contexte mouvant touche également les pratiques de cybersécurité, remettant en cause des situations établies depuis des décennies. Aujourd'hui, les logiciels sont presque partout. Or, la majorité de produits et services numériques souffre de vulnérabilités. Chacune de ces faiblesses peut permettre à un attaquant de compromettre l'intégrité du programme et de l'exploiter à des fins d'enrichissement personnel ou au service d'acteurs étatiques.

Par conséquent, les vulnérabilités logicielles et leur correction en temps opportun sont devenues une préoccupation sérieuse pour tous les acteurs concernés. Que pouvons-nous faire pour nous protéger ? Qui devrait rechercher les vulnérabilités ? Les fournisseurs ou les utilisateurs devraient-ils en être informés ? Quand et comment ? C'est pour répondre à ces questions que nous avons décidé d'aborder l'évolution nécessaire de la divulgation de vulnérabilités et la coordination de leurs corrections.

Trois dimensions ont été plus particulièrement étudiées dans ce livre blanc qui présente l'analyse, les implications (politiques, organisationnelles, légales) et les principales recommandations pour la conception et la mise en œuvre d'une politique répondant à ce défi majeur :

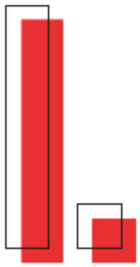
1/ les enjeux de la divulgation de vulnérabilités pour toutes les parties prenantes au regard de l'encadrement juridique et les conséquences de cet encadrement sur les chercheurs éthiques, les responsables de système d'information concernés et les utilisateurs à risque. Un obstacle important à la mise en œuvre des politiques en matière de droits compensateurs dans l'Union européenne est l'absence d'une interprétation unique de ce qui constitue un « piratage » parmi les États membres. Il est ainsi essentiel de fournir la sécurité juridique nécessaire aux chercheurs en sécurité impliqués dans la découverte de vulnérabilités ainsi que d'implémenter des processus appropriés de divulgation ;

2/ les supports technologiques à développer (au sein des organisations) pour accompagner cette évolution forte au travers, notamment, d'un programme structuré de gestion des divulgations bénéficiant d'un fort *sponsorship* et d'un outillage dédié ;

3/ les impacts des changements en matière de maturité des pratiques de cybersécurité, l'accompagnement nécessaire des salariés dans l'utilisation de leurs nouveaux outils et l'évolution des rôles.

L'objectif de ce livre blanc est de proposer une approche constructive et complète grâce à des arguments et des outils permettant un cyberespace moins vulnérable et plus sûr, impulsé par l'Europe. Une telle évolution est d'autant plus importante que le risque de cyberattaques, lié à l'exploitation des vulnérabilités, augmentera inévitablement avec la transformation numérique.

Ce livre blanc propose des mesures législatives et des recommandations concrètes pour toutes les parties prenantes. Cette démarche volontaire consolide l'autonomie technologique des organisations et participe au renforcement de la sécurité en Europe. L'organisation responsable et digne de confiance doit ainsi s'attacher à réduire le risque numérique en valorisant les retours de hackers éthiques. C'est cette nouvelle collaboration qui permettra l'émergence d'une responsabilité de cybersécurité collective.



AVERTIR OU CORRIGER : POURQUOI CHOISIR ?

La question de l'encadrement de la divulgation de vulnérabilités devient de plus en plus pressante au fur et à mesure que croît le nombre de services numériques dotés d'une connectivité (Internet, Bluetooth, etc.). En effet, les vulnérabilités inconnues constituent un risque dont les responsables de système, les éditeurs et leurs exploitants doivent pouvoir prendre connaissance afin de les corriger. Une gestion et une divulgation appropriées des vulnérabilités sont essentielles pour réduire les risques de sécurité numérique.


Partager la connaissance pour réduire le risque
Le pirate, par qui les problèmes arrivent
1/ Il détecte les vulnérabilités d'un système à des fins personnelles, d'espionnage industriel ou pour le compte d'un gouvernement.
2/ Il peut monnayer ses découvertes auprès de l'organisation étudiée ou agir pour le compte de cybercriminels qui exploitent les vulnérabilités et détournent les systèmes à des fins malveillantes.
Agir collectivement pour un cyberespace plus sûr
Au centre de nos vies actuelles, l'espace numérique doit être protégé des actions malveillantes afin de réduire les risques pesant sur les données et les infrastructures. Les organisations peuvent notamment instaurer une collaboration durable avec les hackers éthiques à travers la mise en place d'une politique de divulgation coordonnée de vulnérabilités, permettant une interaction constructive entre toutes les parties prenantes.
L'auditeur du système d'information
1/ Pendant un audit ou dans le cadre d'un programme de *Bug Bounty*, il recherche les vulnérabilités des systèmes d'information à la demande de l'organisation.
2/ Il peut mettre à la disposition des responsables du système des *exploits* pour démontrer l'impact d'une faille.
Le hacker éthique, un expert qui vous veut du bien
1/ Il révèle les failles des systèmes d'information, le plus souvent sans l'autorisation préalable de l'organisation concernée.
2/ Il documente et signale les vulnérabilités identifiées à l'éditeur du service et/ou à son exploitant.
L'éditeur de services numériques
1/ Il évalue et valide les vulnérabilités signalées par ses clients ou le hacker éthique.
2/ Il conçoit les correctifs, s'assure de leur bon fonctionnement et les dissémine à ses utilisateurs.
Le responsable de sécurité, garant d'un cyberespace plus sûr
1/ Il reçoit des hackers éthiques et des auditeurs des rapports d'expertise sur son niveau de sécurité et les vulnérabilités de son système
2/ Il demande la conception de correctifs et veille à leur application.

I/1 Chercher la faille

Alors que nos économies et nos sociétés font leur transformation numérique, elles augmentent leur dépendance au code informatique omniprésent, au travers notamment des ordinateurs et smartphones ou des appareils physiques « intelligents » tels que les compteurs électriques, les équipements hospitaliers, les systèmes de contrôle industriels, les voitures et les appareils électroménagers intelligents.

Nos usages numériques demandent de plus en plus de services. Ceux-là stimulent la création de nouveaux langages de programmation et boostent presque frénétiquement l'évolution des infrastructures. Les approches de gestion et opération s'en trouvent bouleversées. La collecte de données, liées aux utilisateurs et à leurs activités, est devenue quotidienne, permettant de mieux adapter les services aux besoins.

Ces tendances résultent en une augmentation de complexité technique, légale et opérationnelle. En effet, l'appareil législatif, qu'il soit national ou européen, tente de s'étoffer pour mieux encadrer et réguler les usages actuels, anticipés et la transition entre eux.

À ce « mille-feuille » s'ajoutent les menaces et vulnérabilités inhérentes à toute activité humaine et à tout service dématérialisé. Celles-ci, ainsi que les usages malfaisants, conscients (*malwares*) ou non (mésusage de données à caractère personnel), constituent un risque latent pour toute organisation.

DE QUOI PARLE-T-ON QUAND ON DIT…

Vulnérabilité
Une faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser.

Menace
Cause **potentielle** d'un incident de sécurité ou d'une violation de données à caractère personnel pouvant entraîner des dommages sur un bien si cette menace se concrétisait.

Exploit
Tout ou partie d'un programme permettant d'utiliser une vulnérabilité ou un ensemble de vulnérabilités d'un logiciel à des fins malveillantes. Un *exploit* permet également de faire un PoC (*Proof of Concept*, soit une preuve de concept) pour démontrer concrètement la manière de mobiliser une vulnérabilité et son impact négatif sur le système d'information concerné.

Attaque
Action malveillante destinée à porter atteinte à la sécurité d'un bien. Elle représente la **concrétisation d'une menace** et nécessite l'**exploitation d'une vulnérabilité**.

Les systèmes d'information seront d'autant mieux protégés que les vulnérabilités sont découvertes et traitées.

Ainsi, la question de l'encadrement de la divulgation de vulnérabilités devient de plus en plus pressante au fur et à mesure que croît le nombre de services numériques dotés d'une connectivité (Internet, Bluetooth, etc.). Cette question n'est pas nouvelle : depuis que nous créons des produits et services numériques, le sujet de la divulgation de vulnérabilités a suscité des débats au sein de la communauté de la sécurité de l'information.

Créer un logiciel répondant parfaitement à toutes les exigences de sécurité est cependant une gageure. C'est pourquoi, il est crucial d'identifier et corriger les vulnérabilités le plus rapidement possible pour prévenir leur mobilisation par des personnes mal intentionnées. Les systèmes d'information seront d'autant mieux protégés que les vulnérabilités sont découvertes et traitées.

La divulgation de vulnérabilités doit être coordonnée pour être responsable. Il s'agit là d'une opportunité de responsabiliser les différentes parties prenantes. L'ensemble des fournisseurs de services numériques, aussi bien privés que publics, est responsable non seulement du développement des meilleurs logiciels possible, mais également de la gestion responsable des vulnérabilités chaque fois qu'elles sont repérées.

I/1.1 Découvrir une vulnérabilité

Identifier une défaillance est à la portée de beaucoup de personnes et, souvent, sans que cela nécessite une expertise technique poussée. Des cyberdélinquants le font, cherchant à exploiter ces faiblesses à des fins pécuniaires ou d'espionnage. Certains gouvernements constituent des « caches » leur permettant de mobiliser des vulnérabilités pour développer des cyber-armes offensives.

Ainsi, il n'est pas nécessaire de travailler au sein d'une société pour découvrir un dysfonctionnement entraînant un risque de sécurité. Une vulnérabilité est souvent signalée par des personnes bien intentionnées qui chercheront à avertir l'organisation concernée du problème pour qu'elle le corrige. Il est, toutefois, beaucoup plus délicat pour une personne externe à l'organisation de signaler cette vulnérabilité.

Que faire dans ce cas ? Cette zone grise est dangereuse pour la personne qui la découvre et complexe à naviguer pour l'organisation concernée. Un cas fréquent est l'identification d'une défaillance par quelqu'un qui s'est introduit dans un système d'information (SI) de manière illégitime. La notification au responsable du SI peut notamment intervenir en privé, avec ou sans période de grâce pour la correction, avant la divulgation publique. Ou bien, le responsable du SI apprend que la vulnérabilité existe par le biais des réseaux sociaux.

AUDITEUR, CHASSEUR DE BUGS, HACKER ÉTHIQUE : DES ALLIÉS QUI VOUS VEULENT DU BIEN

Des chercheurs en sécurité de l'information, agissant pour améliorer la sécurité des systèmes d'information, existent. Dans le cadre d'un audit de sécurité ou d'un programme de *Bug Bounty*, le chercheur en sécurité n'encourt pas de poursuite judiciaire, car il agit avec l'accord explicite et documenté du responsable du système d'information. Dans ce cadre, les chercheurs éprouvent la sécurité de services numériques avec la permission explicite du responsable du système (le plus souvent *via* un mandat d'audit) et l'informent des vulnérabilités identifiées et des risques qu'elles comportent. Un « blanc-seing » similaire existe dans le cas où des hackers éthiques partent à la chasse des vulnérabilités dans le cadre de programmes de *Bug Bounty*. Il ne s'agit donc pas d'un cas problématique du point de vue de la légalité.

CEUX PAR QUI LES PROBLÈMES ARRIVENT

Agissant dans un cadre d'illégalité, de nombreux cyberdélinquants s'affairent à la création de logiciels malveillants et à leur vente. Ces personnes ne recherchent pas des vulnérabilités pour contribuer à améliorer la sécurité des systèmes d'information, mais plutôt pour les exploiter et/ou les vendre à d'autres acteurs malfaisants. Ces cyberdélinquants s'intéressent ainsi notamment à des *0day (zero day)*, à savoir des vulnérabilités encore inconnues du concepteur, n'ayant été ni préalablement répertoriées, ni publiées.

Ces vulnérabilités *0day* sont souvent difficiles à identifier, requérant ainsi une expertise technique importante, et sont à forte valeur, aussi bien stratégique que pécuniaire, de par les opportunités d'exploitation qu'elles offrent. Ces vulnérabilités peuvent être vendues au prix fort, notamment à des gouvernements qui souhaitent les acquérir pour leurs activités de renseignement et d'armement offensif. Selon l'Agence de sécurité européenne (ENISA), le prix de vente d'une *0day* de choix à un gouvernement varie entre 50 000 et 300 000 dollars.

La divulgation de vulnérabilités doit être coordonnée pour être responsable.

I/**1.2** Le devenir d'une vulnérabilité : avertissement et réception

On ne peut parler de divulgation de vulnérabilités sans s'intéresser aux motivations des personnes signalant les défaillances d'un système d'information. Sont-ils motivés par la volonté d'accroître la sécurité d'un système ? Ou souhaitent-ils profiter de cet avantage pour faire pression sur l'organisation pour leur propre bénéfice sonnant et trébuchant ? Selon la réponse apportée à cette question, des sanctions judiciaires peuvent s'appliquer.

Une difficulté régulièrement observée est l'absence de canal de communication clair et sécurisé permettant une remontée de vulnérabilités effective. En effet, la majorité des organisations dotées d'une présence en ligne n'ont pas de canal dédié aux signalements de défaillances du système d'information. Ce qui explique en partie que, trop souvent encore, l'organisation concernée reste muette face aux signalements de personnes bienveillantes, silence mettant en danger les utilisateurs du service vulnérable.

Cette conception tient également ainsi compte du temps de correction. En effet, rendre tous les détails d'une vulnérabilité publics est nécessaire pour permettre une réévaluation du risque par les utilisateurs. Toutefois, cette démarche ne peut se faire à n'importe quel moment. Une divulgation, sans anticiper les délais de correction, peut aussi entraîner des conséquences négatives pour les utilisateurs.

Ces questions soulignent la nécessité d'une procédure de prise de décision transparente et fluide. Elle est le garant de la sécurité numérique des individus et des acteurs privés et publics, et préserve l'état de droit en ligne.

Comme on le constate quasi quotidiennement, la situation d'un découvreur de vulnérabilités, employant des moyens parfois illégitimes, est complexe à appréhender d'un point de vue organisationnel et juridique. Si le découvreur utilise des moyens illégitimes pour atteindre un objectif louable (améliorer la sécurité d'un système), l'organisation concernée devrait-elle le poursuivre en justice ? Les lois et les pratiques varient grandement et sont, plus ou moins, bienveillantes à l'égard des découvreurs.

Cette hétérogénéité en matière de responsabilités crée des dysfonctionnements majeurs. L'enjeu est donc d'amener un hacker trouvant une vulnérabilité à la signaler au responsable du système afin que ce dernier puisse la corriger et limiter les risques utilisateur liés, sans que cette démarche porte préjudice au hacker.

Il est donc nécessaire de mettre en place un système de divulgation des vulnérabilités, bénéfique pour toutes les parties prenantes. On parle alors de divulgation coordonnée de vulnérabilités ou CVD *(Coordinated Vulnerability Disclosure)*, c'est-à-dire un processus structuré de coopération au cours duquel les vulnérabilités sont rapportées au responsable du système d'information concerné. Nous y reviendrons.

I/**1.3** Organiser un processus structuré de divulgation

Un processus de CVD peut être implémenté au sein d'une entreprise ou d'un organisme public pour permettre un signalement direct de la vulnérabilité à l'entité concernée. Il peut également impliquer un acteur intermédiaire. Dans les deux cas, il s'agit de divulgation coordonnée de vulnérabilités.

La divulgation coordonnée de vulnérabilités donne ainsi à l'organisation l'opportunité de remédier à la défaillance, avant que l'information détaillée de cette dernière ne soit révélée à une tierce partie ou au grand public, avec toutes les implications néfastes que cela peut entraîner.

I/2 La divulgation coordonnée de vulnérabilités (CVD) : modèles et encadrement

La divulgation coordonnée de vulnérabilités est le système le plus à même de protéger à la fois les intérêts du chercheur en sécurité, ceux du responsable du système et ceux des utilisateurs du service numérique affecté. Ce livre blanc vous propose un tour d'horizon des multiples formes que prend la CVD en fonction des pays et organisations. Nous avons exploré ses déclinaisons pour mieux en saisir les impacts.

I/2.1 Une approche internationale

Ainsi, la divulgation de vulnérabilités est un processus par lequel les fournisseurs (de services numériques, qu'ils en soient les créateurs ou les exploitants) et les chercheurs en sécurité peuvent travailler en collaboration pour trouver des solutions qui réduisent les risques associés à une vulnérabilité. Ce processus comprend des actions telles que le signalement, la coordination et la publication d'informations sur une vulnérabilité et sa résolution.

I/2.1.1 Prise de conscience globale

Les vulnérabilités inconnues (dont les *0day*) constituent un risque dont les éditeurs de logiciels et leurs exploitants doivent pouvoir prendre connaissance afin de les corriger. Plus important encore, elles représentent également un marché pour nombre d'entreprises, et plus encore un élément stratégique déterminant pour les capacités défensives et offensives des États.

C'est pourquoi, la question des exportations de logiciels exploitant des vulnérabilités est au cœur des discussions internationales qui accompagnent l'Arrangement de Wassenaar depuis plusieurs années. Ils concernent notamment les biens et technologies à double usage (BTDU). En parallèle, les questions relatives aux cyber-armements font face aux mêmes débats.

L'Arrangement repose sur le volontariat politique des États signataires et prévoit la réglementation de BTDU numériques depuis 2013. Suite à une révision en 2017, Wassenaar prévoit l'encadrement des outils qui permettent de commander le *malware* à distance.

LE PARTAGE D'INFORMATIONS SUR LES VULNÉRABILITÉS : UN ENJEU POUR LA SÉCURITÉ NATIONALE

La recherche et la divulgation de vulnérabilités, notamment de failles *0day*, sont des questions importantes pour les États. Il est difficile de reprocher aux États de vouloir se doter de cette connaissance, car elle leur permet d'acquérir un certain avantage en matière de défense des intérêts nationaux. Cependant, le manque de transparence et le risque de voir privilégier le développement d'un moyen offensif plutôt qu'une sécurisation de l'espace numérique ne peuvent perdurer. En effet, les États sont également garants de l'état de droit, à l'intersection entre intérêts nationaux, privés et particuliers.

La notion de VEP *(Vulnerabilities Equity Process)* existe afin d'apporter une solution à ces questionnements. Il s'agit de la doctrine d'appréciation d'un État lorsqu'il doit décider de divulguer ou non l'existence d'une vulnérabilité. Plusieurs critères sont pris en compte, avec une évaluation des intérêts nationaux en matière de renseignement et de défense face aux intérêts publics.

Cette approche est principalement anglo-saxonne. Les États-Unis sont les premiers à avoir communiqué sur ce point, avec une déclassification partielle de leur doctrine fin 2017. Aucun document relatif à une position sur le sujet n'est publié en France, même si l'on peut spéculer que des discussions afférentes existent. La question de développer des procédures de divulgation coordonnée de vulnérabilités de la part des agences gouvernementales est de plus en plus prégnante. Quel que soit l'état d'avancement de ce type de discussions, il s'agit d'un sujet sensible dont les administrations devront se saisir rapidement étant donné la tension internationale et une menace numérique toujours plus présente.

Le principal problème réside, toutefois, dans le caractère intangible de ces éléments, qu'il s'agisse de la transmission de la connaissance d'une vulnérabilité ou celle de l'*exploit* lui-même. Ainsi, le principal moyen de détection et de contrôle est une approche harmonieuse en matière de divulgation de vulnérabilités.
C'est également le sens de l'Appel de Paris. Ce dernier, lancé le 12 novembre 2018, marque une volonté politique forte de rassembler la communauté internationale pour garantir la paix et la sécurité dans l'espace numérique.

Constitué de neuf Principes, l'Appel de Paris consacre, dans son Principe n° 5, la priorité d'élaborer des moyens pour empêcher la prolifération de pratiques informatiques destinées à nuire et de logiciels malveillants. Il s'agit là d'une ambition de voir se généraliser les pratiques de partage d'information sur les vulnérabilités entre les États.

I/**2.1.2** Objectifs de la CVD

Deux standards internationaux existent et proposent un modèle de la divulgation coordonnée de vulnérabilités : ISO/IEC 29147 et ISO/IEC 30111. Le premier décrit la divulgation de vulnérabilités, tandis que le second aborde les processus de gestion de vulnérabilités remontées. Ces deux standards décrivent un modèle complet des différents aspects de la divulgation coordonnée de vulnérabilités.

Comme explicité dans le standard ISO/IEC 29147, la divulgation de vulnérabilités permet d'accomplir différents objectifs complexes :

1/ veiller à la correction des défaillances ;

2/ minimiser les risques liés à la mobilisation par des acteurs malintentionnés des vulnérabilités identifiées par des acteurs malintentionnés ;

3/ fournir aux utilisateurs des informations suffisantes pour évaluer les risques pour leurs systèmes.

La divulgation de vulnérabilités est un processus et non un événement. En effet, il commence par une prise en compte de la vulnérabilité et continue en cherchant à anticiper les actions à entreprendre en cas de remontée de vulnérabilités. C'est également dans le cadre de ce processus que se décident des questions pertinentes : qui doit savoir, quelle granularité de détail, temps de la communication, etc.

Un PoC illustre concrètement l'impact négatif d'une vulnérabilité.

Le processus de divulgation de vulnérabilités connaît deux approches extrêmes.
D'une part, il existe la divulgation complète, à savoir la communication publique de tous les détails de la vulnérabilité, souvent sans aucune mesure d'atténuation pour protéger les utilisateurs. C'est ce que l'on peut observer par exemple sur les réseaux sociaux. Un exemple récent de cette démarche est la publication d'une vulnérabilité *0day* affectant le système d'exploitation Windows 10 par un utilisateur de Twitter avec l'alias SandboxEscaper. La personne avait également essayé de vendre la vulnérabilité et un PoC d'*exploit* sur différents forums avant de se raviser et de publier le PoC sous son compte GitHub. SandboxEscaper a récidivé, quelques semaines plus tard, publiant directement le PoC d'une vulnérabilité Windows 10 différente sur GitHub.

D'autre part, une personne ayant identifié une vulnérabilité peut opter pour l'approche totalement contraire, soit ne recourir à aucune divulgation. Dans ce cas-là, rien n'est divulgué. Il est ainsi possible, par exemple, à un gouvernement ou à des vendeurs de vulnérabilités d'en acquérir pour exploitation ou avantage à un stade ultérieur.

Aucune de ces approches n'est acceptable pour les organisations et utilisateurs concernés. *A contrario*, la divulgation coordonnée de vulnérabilité est la modalité qui donne les meilleurs résultats.
Ainsi, la CVD est un processus visant à atténuer, voire à éradiquer, les potentiels impacts négatifs d'une ou plusieurs vulnérabilités. Le processus de divulgation coordonnée de vulnérabilités peut être défini comme suit :

« Le processus de collecte d'informations auprès des chercheurs de vulnérabilités, de coordination du partage de ces informations entre les parties prenantes concernées et de divulgation de l'existence des vulnérabilités et de leur atténuation à diverses parties prenantes, y compris le public ».

Comme illustré ci-dessous, la contribution des parties prenantes à ce processus se fait essentiellement *via* des rapports des pratiques de découverte de vulnérabilités. Sous la forme de correctifs, ces derniers sont enregistrés en bases de données standardisées et partagées au sein de la communauté de cybersécurité.

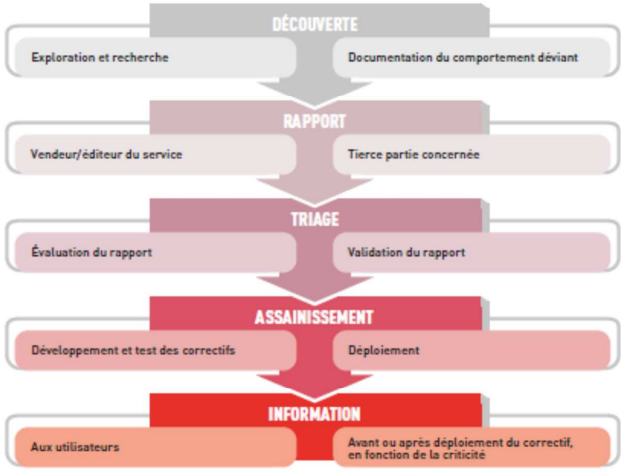
I/2.1.3 Processus et formalisation de la CVD

D'après ISO/IEC 30111, différentes phases du processus de divulgation peuvent être identifiées.

La vulnérabilité peut se voir attribuer un identifiant CVE *(Common Vulnerabilities and Exposures)* par le MITRE, organisation étatsunienne à but non lucratif travaillant en défense des intérêts publics. Un identifiant CVE, associé à une vulnérabilité, suppose que celle-ci ait été identifiée, et permet au MITRE de la classer dans une base de données de vulnérabilités recensées. Cette base inclut également les dates auxquelles ces vulnérabilités ont été découvertes, si l'alerte est toujours en cours ou si la vulnérabilité a été corrigée.

Ce modèle standard n'est cependant pas décliné de façon harmonieuse dans les différentes juridictions et par les acteurs concernés. Il n'existe ni de définition harmonisée de ce qu'est un accès illégitime à un système d'information, ni de protection minimale commune des hackers éthiques. Par conséquent, les législations nationales sont disparates, avec peu, voire aucune, coordination supra-étatique.

Phases du processus de divulgation



I/2.2 Encadrement national : les cas les plus notables

La divulgation coordonnée de vulnérabilités est le processus le plus à même de protéger à la fois les chercheurs en sécurité, les responsables de système d'information, les tiers impliqués dans la fourniture du service concerné, et les utilisateurs du service vulnérable. Certains pays ont commencé à aborder le sujet de la CVD au niveau national, visant à réduire l'hétérogénéité des pratiques des différents acteurs, privés et publics, opérant sur le territoire.

I/2.2.1 Le modèle français : un encadrement incomplet

En France, l'article 323-1 du Code pénal dispose que l'intrusion et le maintien illégitimes dans un système d'information sont punis (par amendes et emprisonnement). Le cadre réglementaire a évolué avec l'adoption de l'article 47 de la Loi pour une République numérique du 7 octobre 2016. Il inscrit la possibilité de rapporter une vulnérabilité à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sans craindre de poursuites de la part du procureur de la République, à condition pour le divulgateur d'être de *« bonne foi »*. Le site web de l'ANSSI contient une rubrique spéciale dédiée à la divulgation de vulnérabilités.

Cette mesure permet ainsi aux hackers utilisant des moyens illégitimes d'échapper à la qualification d'infraction. L'inscription d'une telle démarche dans une loi régissant la confiance et l'économie à l'ère du numérique, souligne la prise de conscience de l'importance de la divulgation de vulnérabilité et de la nécessité de l'encadrer pour le bien de tous. L'article 47 propose, en conséquence, un cadre légal pour l'implémentation d'un processus de divulgation coordonnée de vulnérabilités.

Malgré cette prise de conscience, un examen critique de l'article 47 montre ses limites en ce qui concerne la protection des hackers éthiques. En effet, les poursuites judiciaires sont toujours possibles. La rédaction de cet article sous-entend que le chercheur en sécurité ne doit ni contacter le responsable du système d'information concerné directement, ni divulguer la vulnérabilité à qui que ce soit d'autre que l'ANSSI. La protection accordée par l'article L2321-4 du Code de la défense est conservée dans ce cadre seul.

« L'amendement Bluetouff » (voir encadré ci-contre) a finalement été rejeté par l'Assemblée nationale, laissant ainsi l'article 47 comme seule protection pour les hackers bien intentionnés. Par conséquent, celui-ci doit obligatoirement s'adresser à l'ANSSI et ne peut pas alerter le responsable du système directement.

En outre, l'article 47 ne protège que des poursuites engagées par le procureur de la République sur dénonciation d'un agent public, mais pas de celles engagées par le responsable du système concerné par la vulnérabilité. Ce dernier peut donc engager des poursuites à l'encontre d'un hacker bien intentionné. L'article 323-1 du Code pénal est toujours applicable aux chercheurs, même s'ils sont de *« bonne foi »*.

L'immunité pénale totale a été refusée par le législateur français, de même que les propositions d'une immunité concernant uniquement les infractions d'accès et de maintien frauduleux dans un système d'information. Plus spécifiquement, les infractions de modification ou de suppression des données ne font pas partie des exclusions envisagées, afin d'éviter qu'un hacker malveillant ne s'introduise dans un système, n'y injecte des *malwares* et ne se targue ensuite d'avoir découvert une vulnérabilité.

En plus des poursuites dans le domaine pénal, les chercheurs en sécurité sont également susceptibles d'être poursuivis sur les fondements notamment du droit civil, du droit des contrats, du secret des affaires, de la propriété intellectuelle.

« L'AMENDEMENT BLUETOUFF »

En janvier 2016, plusieurs députés français, issus du groupe parlementaire Les Républicains, souhaitaient une protection accrue des hackers éthiques, ce qui les avait amenés à proposer « l'amendement Bluetouff ». Ce dernier ajoutait un nouvel alinéa à l'article 323-1 du Code pénal, ainsi rédigé : *« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »*

Cet amendement tirait son nom de l'arrêt « Bluetouff » de la Chambre criminelle du 20 mai 2015. Olivier Laurelli, blogueur connu sous le pseudonyme Bluetouff, est condamné en février 2014 par la Cour d'appel de Paris pour maintien frauduleux dans un système d'information, ainsi que pour vol de fichiers à l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses). L'Anses ayant un défaut de sécurisation de son site web et donc de ses données, Olivier Laurelli a pu accéder à des fichiers confidentiels par le biais d'un moteur de recherche.

En remontant l'arborescence du site, Olivier Laurelli était tombé sur une page demandant une authentification : le blogueur savait donc qu'il se maintenait dans le système d'information de manière irrégulière. Il a également fait une copie de nombreux fichiers, dont il a publié une partie sur son site, action valant divulgation des défaillances. Relaxé en première instance, Olivier Laurelli est finalement condamné par la Cour d'appel à 3 000 euros d'amende pour *« maintien frauduleux dans un système de traitement automatisé de données »* (soit condamnation au titre de l'article 323-1 du Code pénal) et *« soustraction de données »* (soit condamnation au titre de l'article 311-1 du Code pénal). Son pourvoi en cassation est rejeté.

I/**2.2.2** Les Pays-Bas « dédramatisent » la divulgation de vulnérabilités

Le modèle néerlandais est souvent considéré comme une réussite en raison des nombreux signalements de vulnérabilités effectués dans le cadre des politiques de divulgation mises en place par les organisations, tant privées que publiques. Il crée un environnement plus protecteur pour les hackers éthiques. En effet, chaque politique de divulgation de vulnérabilités explique sous quelles conditions un chercheur n'encourra pas de poursuites judiciaires (tant pénales que civiles).

Dès janvier 2013, le Nationaal Cyber Security Centrum (NCSC), soit l'Agence néerlandaise de cybersécurité, a publié des lignes directrices relatives à la politique de divulgation de vulnérabilités et essentiellement destinées aux responsables de sécurité. Elles assistent une organisation dans la création de sa propre politique de CVD. Différentes entreprises, notamment du secteur des télécommunications, ont également suivi l'effort en publiant leurs politiques de CVD.

La divulgation de vulnérabilités fait partie des recommandations principales du NCSC pour une cyber-résilience, et est ainsi perçue comme une activité parmi d'autres pour un professionnel de sécurité. Cette volonté de « dédramatiser » s'adresse aussi aux hackers éthiques, comme l'illustre la première page du document. Elle montre, en effet, le buste d'un jeune homme arborant fièrement un T-shirt sur lequel est inscrit « J'ai piraté le gouvernement néerlandais et tout ce que j'ai eu, c'est ce T-shirt pourri » *(I hacked the Dutch government and all I got was this lousy t-shirt)*.

D'après ces lignes directrices, il doit y avoir le moins d'intermédiaires possible entre la personne qui signale une vulnérabilité et la personne en charge de résoudre le problème au sein de l'organisation concernée. Néanmoins, si une vulnérabilité affecte plusieurs systèmes, il est judicieux d'informer plusieurs parties. Le NCSC ou d'autres acteurs de la communauté peuvent alors jouer un rôle de coordination.

La publication de ces lignes directrices par le NCSC a été positivement accueillie par le Procureur néerlandais. En effet, le bureau du Procureur a informé tous les départements judiciaires de cette évolution du cadre légal. L'explication insiste sur le fait que, si le hacking éthique n'est pas reconnu en tant que tel dans la loi néerlandaise, la dimension éthique doit être un facteur de premier plan lorsqu'il s'agit de déterminer si une action constitue une violation de la législation pénale.

Cette interprétation, déclinée en arbre de décision (ci-dessous), permet de traiter les éventuelles zones grises de la loi quant au suivi à donner aux remontées de vulnérabilités. Si un hacker trouve une vulnérabilité et la signale au responsable du système, cela constitue *a priori* un acte de hacking éthique. En revanche, si des indices suggèrent que le hacker a dépassé le simple signalement de la faille (par exemple, s'il y a eu copie de données sensibles), une enquête criminelle doit avoir lieu.

Arbre de décision, proposé par le procureur néerlandais, pour qualifier pénalement un cas de divulgation de vulnérabilité

I/2.2.3 Les États-Unis : un précurseur aux pieds d'argile

Aux États-Unis, les entreprises ont commencé à publier leurs politiques de divulgation au début des années 2010. Les agences fédérales ont alors emboîté le pas pour faciliter la mise en place de politiques de divulgation, tant dans les organisations privées que publiques. En 2015, l'Agence fédérale des télécommunications *(National Telecommunication and Information Administration)* a réuni les parties prenantes du processus de divulgation pour rédiger un modèle de divulgation coordonnée de vulnérabilités. Ce modèle visait à aider les organisations à entreprendre la création de leurs propres politiques de CVD.

D'autres agences fédérales ont suivi, telles que la Commission fédérale du commerce, l'Agence des produits alimentaires et médicamenteux et l'Agence de la sécurité routière. Le Département de la défense a rejoint la tendance en publiant en 2016 une politique de divulgation de vulnérabilités.

Les lois américaines n'ont pas été modifiées depuis l'émergence de ces politiques, mais leur interprétation et leur application diffèrent aujourd'hui. La loi anti-hacking *(Computer Fraud and Abuse Act* ou CFAA) est toujours utilisée pour protéger les systèmes d'information américains. Néanmoins, le Département de la justice a publié des orientations pour que les procureurs fédéraux s'assurent que les poursuites n'aient lieu que dans le cas où elles servent un *« intérêt fédéral substantiel »*. De même, l'Office de droit de la propriété intellectuelle a recommandé des exemptions à la loi idoine, le DMCA *(Digital Millennium Copyright Act*, la loi américaine visant à réguler le droit d'auteur à l'ère du numérique).

Ces efforts semblent toutefois insuffisants. Ainsi, fin novembre 2019, l'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) du Département de la sécurité intérieure a annoncé préparer une directive exigeant de toutes les agences fédérales la création et la publication d'une politique de divulgation de vulnérabilités. Selon la CISA, la plupart des agences fédérales ne dispose d'aucun mécanisme officiel pour recevoir des informations provenant de tiers concernant les vulnérabilités potentielles de sécurité de leurs systèmes, et beaucoup n'ont pas de stratégie définie pour traiter les rapports lorsqu'ils arrivent.

Cette démarche s'inscrit dans une focalisation croissante du gouvernement américain sur la divulgation de la vulnérabilité, comme en témoigne le projet de politique de CVD du Bureau de la gestion et du budget (OMB), qui obligerait toutes les agences fédérales à publier une politique de divulgation de vulnérabilités dans un délai de 180 jours.

I/2.3 Un paysage européen fragmenté

Le caractère transfrontalier de la création et diffusion de services numériques peut complexifier le choix de la juridiction compétente en cas de litige. Un nombre croissant d'aspects, liés à l'autonomie technologique, se discute au niveau de l'Union européenne plutôt qu'au niveau national. Aborder la divulgation coordonnée de vulnérabilités sous un angle purement national semble ainsi lacunaire. Malgré cette dimension européenne, les initiatives existantes restent encore limitées.

EN DÉFENSE DES HACKERS ÉTHIQUES DES AMÉRIQUES

Malgré différents changements d'interprétation et d'application de lois fédérales américaines, la protection des hackers éthiques est considérée comme insuffisante par l'EFF *(Electronic Frontier Foundation)*, célèbre association américaine de défense des droits numériques. En effet, l'EFF demande des amendements au CFAA et a lancé un projet de plaidoirie en ce sens.

L'argument de l'EFF est que le code informatique est une forme d'*« expression d'idées sous une forme claire et précise »* et doit être protégée en tant que telle au titre de la Convention américaine des droits humains. Plus spécifiquement, la divulgation de vulnérabilités est considérée comme une forme d'expression : *« Comme toutes les activités productrices de connaissance, la recherche en matière de sécurité dépend de la libre circulation de l'information et de l'échange d'idées sans entrave. Un sous-ensemble particulier de ces recherches traite de la découverte, de la notification et de la résolution des vulnérabilités des systèmes d'information. Découvrir les failles de sécurité est tout aussi important que de signaler les résultats afin que les utilisateurs puissent se protéger et que les fournisseurs puissent réparer leurs produits. Pour cette raison, les lois ne devraient pas criminaliser la démonstration et la divulgation de vulnérabilités. »*

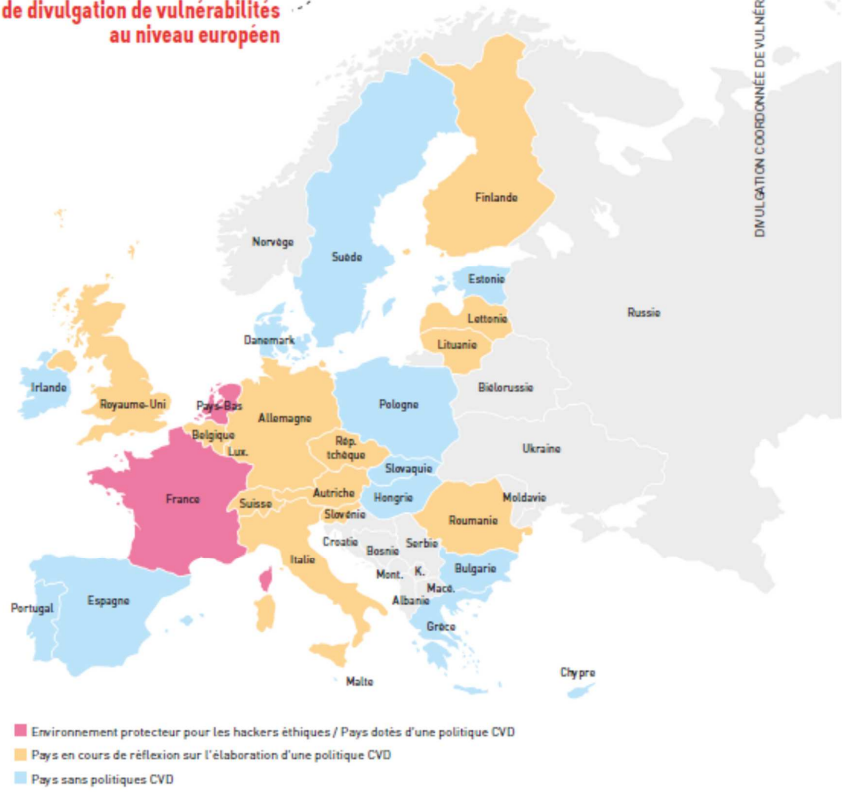
I/2.3.1 Un intérêt extrêmement hétérogène pour la CVD

Comme nous l'avons vu plus tôt, la France et les Pays-Bas sont les seuls à s'être dotés d'une politique de divulgation coordonnée de vulnérabilités générale, valable pour tous les secteurs d'activité. La Lituanie est un cas spécifique car le pays balte a établi un cadre de divulgation de vulnérabilités pour un secteur en particulier : les fournisseurs de réseaux de communication publique.

D'autres États membres, en orange ci-dessous, ont amorcé des efforts en ce sens. Il en est de même pour la Suisse : bien qu'elle ne soit pas un État membre de l'Union européenne, elle fait partie du Marché unique numérique.

Enfin, plusieurs États membres n'ont toujours pas amorcé d'efforts pour créer et promouvoir une politique de CVD en bleu ci-dessous.

La mise en place de politique de divulgation de vulnérabilités au niveau européen



Environnement protecteur pour les hackers éthiques / Pays dotés d'une politique CVD

Pays en cours de réflexion sur l'élaboration d'une politique CVD

Pays sans politiques CVD

I/2.3.2 L'absence de législation européenne en matière de protection des hackers de bonne foi

En droit européen, la Directive 2013/40/UE du 12 août 2013, dite « Directive Cybercrime », propose un socle minimal en ce qui concerne la répression des cyber-infractions (article 3) :

« Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, lorsqu'il est intentionnel, à tout ou partie d'un système d'information, lorsque l'acte est commis en violation d'une mesure de sécurité, au moins lorsqu'il ne s'agit pas de cas mineurs. »

L'article 323-1 du Code pénal français est la transposition de cet article 3.

La Directive Cybercrime ne mentionne aucune exemption de poursuites judiciaires pour les hackers bien intentionnés. Les États membres ne sont donc pas tenus d'en introduire une dans leur législation nationale.

I/2.3.3 Un cadre européen incomplet mais voué à évoluer

Malgré une politique européenne timide en matière de divulgation de vulnérabilités, la CVD fait progressivement son apparition dans l'arsenal politico-législatif européen. L'Union européenne a ainsi initié, par le biais de l'Agence européenne de la cybersécurité (ENISA), la création d'outils pour inciter les acteurs privés et publics à mettre en place des politiques de divulgation. En 2015, l'ENISA a ainsi publié un guide de bonnes pratiques en matière de divulgation de vulnérabilités.

Ce dernier encourage les entités publiques et privées à mettre en place leur propre politique de divulgation de vulnérabilités. Il explique notamment que les CERT (*Computer Emergency Response Team*, l'équipe dédiée de la réponse à incidents de sécurité) nationaux ont un rôle à jouer dans le processus de divulgation, même s'il est préférable que le hacker cherche premièrement à contacter le responsable du système. Contacter un CERT est opportun si le hacker n'a pas le contact du responsable du système ou si la vulnérabilité concerne de multiples organisations.

En parallèle, le programme de financement européen Horizon2020 pour la recherche et le développement, soutient la recherche dans le domaine de la divulgation de vulnérabilités. Ainsi, le consortium européen SPARTA compte parmi ses 44 membres fondateurs YesWeHack, portant de fait un axe notable de recherche sur les programmes de divulgation coordonnée de vulnérabilités.

Au-delà de ces politiques incitatives non contraignantes, l'Union européenne commence également à légiférer sur le sujet. Ainsi, le *Cybersecurity Act*, règlement européen entré en vigueur au printemps 2019, marque une étape importante vers une diffusion plus large de politiques de divulgation coordonnée de vulnérabilités au sein des entreprises. Même si ce n'est pas le thème central du règlement, le texte promeut le rôle de la divulgation coordonnée de vulnérabilités pour améliorer la cybersécurité (Considérant 30). Ainsi, le *Cybersecurity Act* dispose que l'une des missions de l'ENISA est d'assister les États membres, les institutions, organes et organismes de l'Union dans l'établissement de politiques de divulgation de vulnérabilités (art. 6 §1).

Outre la définition de la mission de l'ENISA, le *Cybersecurity Act* propose un cadre de certification de cybersécurité pour harmoniser, à l'échelle européenne, les méthodes d'évaluation et les différents niveaux d'assurance de la certification. Le nouveau schéma européen de certification de cybersécurité ainsi défini devra comporter des règles concernant le signalement et la gestion de vulnérabilités (art. 54 §1m). Plus précisément, l'éditeur ou fournisseur d'un produit, service ou processus certifié doit fournir les informations de contact, ainsi que les méthodes acceptées pour la réception d'informations sur les vulnérabilités de la part des utilisateurs ou des chercheurs en cybersécurité (art. 55 §1c).

Ces dispositions signifient qu'un fabricant ou fournisseur devra *a minima* disposer d'une ébauche de politique de divulgation de vulnérabilités s'il souhaite certifier ses solutions. Le *Cybersecurity Act* ne liste pas d'exigences spécifiques relatives au type de politique de divulgation de vulnérabilités qu'une organisation doit mettre en place. On peut supposer que chaque schéma de certification détaillera plus amplement les exigences en la matière.

I/3 Les enseignements à tirer

La complexification des technologies, permettant de créer des produits et services numériques de plus en plus sophistiqués, est une source primordiale de facteurs de risques. La connectivité à Internet permet ainsi à une vulnérabilité dans un système d'information de se propager et d'avoir des conséquences transfrontalières. Celles-ci peuvent être dramatiques si la vulnérabilité entraîne des risques majeurs, de par la multiplicité de composants affectés ou encore le nombre important d'utilisateurs touchés.

I/3.1 Un puzzle législatif encore insuffisant

Il est primordial d'encadrer et de structurer la divulgation de vulnérabilités. Différentes approches, à la fois au niveau national et européen, existent pour aborder ce défi. Le modèle français se caractérise par une politique de divulgation de vulnérabilités qui repose essentiellement sur l'intermédiation de l'ANSSI. Promu par l'article 47 de la Loi pour une République numérique, ce modèle, visant à garantir l'anonymat du hacker, est sans doute adapté pour des vulnérabilités relevant de la cybersécurité de l'État. Néanmoins, l'article 47 n'offre pas une protection complète à celui qui trouve la vulnérabilité.

D'autres pays ont fait le choix de favoriser le contact direct entre les chercheurs en sécurité et les responsables de système, sans intermédiaire centralisé. Cette alternative a le mérite de limiter le risque de poursuites judiciaires et d'instaurer une collaboration entre eux. En Europe, les Pays-Bas sont l'exemple le plus flagrant de l'efficacité du modèle désintermédié de divulgation coordonnée de vulnérabilités.

La législation européenne est également lacunaire en matière d'encadrement de divulgation des vulnérabilités. Il n'existe pas de définition harmonisée de ce qu'est un accès illégitime à un système d'information, ni de protection minimale commune des hackers éthiques. Cette absence conduit à des législations nationales hétérogènes en matière de divulgation de vulnérabilités.

Force est également de constater que, malgré le travail exhaustif de l'ENISA pour la création d'un guide de divulgation de vulnérabilités, celui-ci n'a pas eu l'impact espéré. Le sujet est pourtant transfrontalier et appelle une harmonisation minimale qui fournit aux chercheurs en sécurité une protection lorsque ceux-ci contribuent à l'amélioration générale de la sécurité des systèmes.

I/3.2 Des effets de bord inattendus

Le canal de remontée de vulnérabilités n'est pas sans impact. En effet, le modèle français, décrit plus tôt, présuppose une réactivité adéquate de l'ANSSI afin que les vulnérabilités soient traitées dans les meilleurs délais. Le risque majeur d'une telle approche centralisée est que l'ANSSI ne soit pas en mesure d'aiguiller les signalements de vulnérabilités en temps et en heure, ralentissant ainsi la réaction et, donc, la correction.

Tel est, par exemple, le cas au Japon, qui a également mis en place un système centralisé. Au Japon, les chercheurs en sécurité doivent signaler les vulnérabilités à une agence gouvernementale, laquelle se charge conjointement avec le JP-CERT de contacter le vendeur ou développeur, pour coordonner le processus de divulgation. Ce système a été un succès à son origine, au milieu des années 2000. Cependant, depuis plusieurs années, le nombre de signalements a significativement augmenté et le système se retrouve engorgé.

L'effet d'engorgement, surtout lorsqu'un processus de qualification *a posteriori* existe, peut être un véritable problème de diffusion des informations sur les vulnérabilités, rendant ainsi le processus centralisé contre-productif. Ainsi, la base de données étasunienne sur la vulnérabilité des États-Unis (*National Vulnerability Database*, NVD) a un retard significatif en comparaison avec celle de la Chine (*The Chinese National Vulnerability Database* - CNNVD) quant au délai moyen entre la divulgation initiale et l'inclusion dans la base de données (respectivement 33 jours contre 13 jours). La couverture des vulnérabilités incluses diffère également : la CNNVD collecte de façon active des informations relatives aux vulnérabilités sur le web, tandis que la NVD est tributaire des soumissions volontaires des éditeurs de logiciels et chercheurs individuels.

Au-delà de la question de volume, le « mille-feuille » législatif a également ses défis. Le Règlement général pour la protection des données à caractère personnel, RGPD, est entré en application en mai 2018 sur tout le territoire de l'UE. Il vise à harmoniser les législations portant sur la protection des données au sein des États membres et à introduire des règles précises quant à l'implémentation d'outillage permettant l'exercice du droit fondamental à la vie privée en ligne pour les résidents de l'Union. Dans ce cadre-là, différentes préconisations sont édictées touchant, entre autres, à la pseudonymisation des données et à la notification de violations.

Le RGPD crée la nécessité de prévoir des moyens de divulgation en cas de défaut de protection de données à caractère personnel, afin de protéger les chercheurs en sécurité qui s'efforcent de découvrir les abus à encourager les signalements les concernant. Un exemple notable de cette urgence induite par le RGPD est l'anonymisation de données. L'anonymisation est un problème complexe ; c'est pourquoi, le RGPD préconise le recours à la pseudonymisation comme approche de sécurisation moins complexe et plutôt efficace. Mais qu'advient-il lorsqu'un hacker éthique teste la robustesse de la pseudonymisation sur un jeu de données à caractère personnel rendu public ? Si celle-ci est inadéquate, une remontée devra être faite, exposant ainsi le chercheur à des représailles.

PAS VRAIMENT SECRET : L'IMPACT NÉGATIF D'UNE PSEUDONYMISATION DÉFAILLANTE

Divers cas de pseudonymisation inadéquate sont connus. On peut ainsi citer une sélection « anonymisée » de requêtes de recherche, publiée en 2006, par l'opérateur AOL. Par le regroupement des annuaires téléphoniques, elle a révélé des relations, des maladies et des activités criminelles. La même année, Netflix a été poursuivi pour avoir publié des critiques mal anonymisées qui révélaient l'orientation sexuelle, tenue secrète, d'une femme. En août 2017, des chercheurs allemands ont acheté les habitudes de navigation « anonyme » de 3 millions d'Allemands auprès d'un courtier en données et ont réussi à découvrir les habitudes pornographiques d'un juge, les problèmes médicaux d'un député et les détails de différentes affaires pénales en cours.

Enfin, le signalement de violations de données à caractère personnel est une exigence forte du RGPD, devant se faire en délais contraints et requérant des détails sur les données compromises. Lorsqu'une organisation a connaissance d'une violation de données, présentant des risques pour les individus concernés, elle a 72 heures pour la signaler à l'autorité de contrôle (l'autorité administrative indépendante nationale en charge de la protection des données à caractère personnel). Beaucoup d'organisations ne sont pas adéquatement outillées pour recevoir et traiter ce genre de signalements.

En France, l'autorité de contrôle, la CNIL (Commission nationale informatique et libertés), adopte une approche répressive en cas de non-respect de l'obligation de notification dans les 72 h. La Commission rappelle aussi que ce manquement est passible d'une amende de 10 millions d'euros ou 2 % du chiffre d'affaires. Dans ce cadre, toutefois, aucune place n'est prévue pour un signalement d'une violation de données inconnue au responsable identifiée par un chercheur en sécurité, ni à une remontée directe à l'autorité de contrôle par ce même chercheur.

I/3.3 La CVD est un outil essentiel dans la réduction du risque numérique

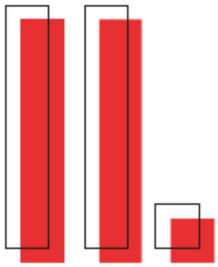
Découvrir une vulnérabilité et l'exploiter au détriment des utilisateurs et du responsable du système d'information présente un avantage incontestable : ces défaillances peuvent être mobilisées pour des attaques ou encore achetées par des acteurs qui peuvent les opérationnaliser à des fins offensives, augmentant le risque de sécurité numérique pour tous les acteurs légitimes.

Cependant, les éditeurs de logiciels ne sont pas seuls dans la course contre de tels acteurs malveillants. Les chercheurs en sécurité sont également actifs dans la lutte contre les vulnérabilités et contribuent à démultiplier les efforts de réduction de risques numériques. C'est pourquoi, il est primordial d'encadrer et de structurer la divulgation de vulnérabilités.

Les chercheurs en sécurité peuvent ainsi contribuer de manière significative à l'augmentation de la sécurité numérique des produits. La plupart des chercheurs souhaitent, en effet, recevoir une sorte de reconnaissance, allant des simples remerciements à la possibilité de communiquer à ce sujet publiquement (par exemple dans des conférences, des publications universitaires, etc.), à des rétributions financières ou à des offres d'emploi.

Et pourtant, au lieu de récompenses, la découverte de vulnérabilités peut exposer les chercheurs à des risques juridiques et à des menaces de poursuites de la part de fournisseurs pour avoir enfreint les conditions de services. Il existe de nombreux cas d'éditeurs de logiciels, de prestataires de services ou encore de responsables de système d'information menaçant les chercheurs de poursuites, pour le signalement d'une vulnérabilité, au lieu de coopérer avec eux pour la corriger le plus rapidement possible.

Une gestion et une divulgation appropriées des vulnérabilités sont donc essentielles pour réduire les risques de sécurité numérique. La communauté technique a développé de bonnes pratiques pour un comportement responsable dans ce domaine. Elle a atteint un certain degré de maturité au fil du temps : la divulgation coordonnée des vulnérabilités (CVD) s'impose donc comme une approche pertinente. Cependant, des obstacles à son adoption à grande échelle existent. De nombreux décideurs ne sont pas encore suffisamment conscients de la nécessité de supprimer ces obstacles et d'encourager un comportement responsable de toutes les parties prenantes. Nous explorerons le « comment faire » dans le prochain chapitre.



MOBILISER L'INTELLIGENCE COLLECTIVE POUR MIEUX (SE) PROTÉGER

Les chercheurs en sécurité peuvent contribuer de manière significative à accroître la sécurité numérique des produits. Cependant, le « premier contact » est difficile à établir. Plus largement, même lorsqu'une vulnérabilité est signalée, les éditeurs peuvent préférer ne pas en tenir compte. Ce silence pousse souvent les chercheurs en sécurité à recourir à la divulgation publique comme un moyen de faire pression sur les éditeurs pour corriger la vulnérabilité.

Alors, comment aborder la découverte et l'interaction en vue de correction d'une vulnérabilité lorsque cette identification est faite par une personne externe à l'organisation ?

Dans ce chapitre, nous présentons les enjeux de la CVD, pour chaque personne et organisation concernée, ainsi que pour l'Union européenne et les États membres. En cohérence avec une démarche constructive, nous proposons également les approches les plus efficaces pour remédier aux insuffisances liées à la mise en place d'une politique de divulgation.

II/**1** Les enjeux de la divulgation coordonnée

Lorsque les acteurs malveillants sont les seuls informés d'une vulnérabilité ou ont un avantage chronologique, le risque de sécurité numérique augmente pour tous les acteurs – des utilisateurs aux tiers jusqu'au fournisseur dont la réputation peut être endommagée – notamment si les vulnérabilités ont des répercussions importantes.

La divulgation coordonnée de vulnérabilités est le processus permettant d'instaurer une collaboration entre le hacker éthique et le responsable du système. Il laisse le temps de remédier à la vulnérabilité avant sa publication. L'adoption de politiques de divulgation coordonnée a donc des bénéfices significatifs pour les parties prenantes : montée en maturité de la sécurité, développement de talents au sein des organisations et autonomie technologique des éditeurs et leurs clients, car ils maîtrisent les risques numériques liés à la gestion des vulnérabilités.

II/**1.1** Faire accroître sa maturité en matière de sécurité

La divulgation de vulnérabilité est un processus et non un événement. Il commence, en effet, par une prise de conscience de la vulnérabilité et continue en posant (au minimum) les deux questions suivantes :

- Que dois-je faire en réponse à une remontée de vulnérabilité ?
- Qui a besoin de savoir ? Quels détails doivent être communiqués et quand ?

Ainsi, la gestion des vulnérabilités remontées exige l'implication de tous les acteurs. Ils doivent prendre des mesures afin de réduire la fenêtre d'exposition des utilisateurs aux risques de sécurité numérique lors de l'utilisation du service affecté.

Comprendre, cartographier, structurer, responsabiliser et rendre opérant un processus, où les rôles et responsabilités des actifs numériques sont clairement identifiés et endossés, n'est pas simple. Pourtant, c'est là une description adéquate d'un processus efficace de divulgation et gestion de vulnérabilités. Par conséquent, l'établissement de ce processus constitue un levier significatif pour faire « mûrir » la sécurité d'une organisation. Afficher une politique de CVD et réagir selon le processus qu'elle définit sont autant d'éléments contribuant à renforcer et consolider la confiance des utilisateurs, partenaires et responsables d'un service numérique.

De manière plus pragmatique, la transparence qu'offre un programme de divulgation coordonnée, clair et aisément accessible, constitue un argument marketing différenciant. Alors que les attaques de rançongiciels et les fuites de données sont tellement fréquentes qu'elles ne sont même plus relatées dans les médias, afficher son engagement pour la réduction des vulnérabilités qui l'affectent renforce la crédibilité d'une organisation.

La divulgation de vulnérabilité est un processus et non un événement.

II/1.2 Développement de talents

Lorsqu'une organisation met en place et applique une politique de CVD, différents métiers sont impliqués. Accueillir de façon constructive les remontées de vulnérabilités, de la part de hackers éthiques, offre aux fonctions concernées la fonction de s'enrichir et de diversifier continuellement leurs compétences. En effet, cela permet de mettre à l'épreuve son travail et de développer ses compétences en sécurité, sur les plans technique et managérial.

En effet, la visibilité des services et produits numériques utilisés par une organisation est une tâche complexe. Le monitoring exhaustif et continu de leurs composants pour s'assurer qu'ils ne souffrent pas de vulnérabilités est une gageure. Or, cette connaissance fine et actuelle des actifs est un prérequis pour une gestion des risques numériques évolutive et pertinente. S'ouvrir à des chercheurs externes, *via* une politique de divulgation coordonnée de vulnérabilités, permet donc une telle visibilité et une telle connaissance, y compris des anciennes versions des logiciels. Il est ainsi possible de concilier une gestion de l'existant avec un développement continu des compétences, indispensable pour faire face à des technologies en constante évolution.

Enfin, la mise en place de processus de CVD permet de responsabiliser les développeurs de solutions numériques et de garantir le respect des exigences de qualité et de sécurité. De même, il leur est possible d'identifier une vulnérabilité dans différentes versions de code, notamment des versions antérieures de la solution toujours utilisées par le client. La montée en compétences se fait, d'une part, en améliorant sa production comme conséquence de la divulgation de vulnérabilités, et d'autre part, *via* une interaction directe et experte avec le chercheur éthique.

II/1.3 Autonomie technologique et maîtrise des risques numériques

Le cycle de vie de la vulnérabilité comprend : sa découverte, la disponibilité des *exploits*, sa divulgation, la disponibilité et l'installation de ses correctifs. La notion de cycle de vie décrit les différents événements susceptibles d'affecter une vulnérabilité et d'influencer le niveau de risque pour les utilisateurs, mais aussi la nécessité d'action de la part des différentes parties prenantes. En outre, une vulnérabilité découverte est susceptible d'être redécouverte par différents acteurs dans un délai relativement court.

Les périodes entre ces événements déterminent les phases pendant lesquelles l'exposition des utilisateurs aux risques varie. Ainsi, elle augmente après la découverte d'une vulnérabilité par des acteurs malveillants et s'intensifie dès lors qu'un *exploit* a été développé. Puis, elle diminue lorsque la vulnérabilité est révélée (car des mesures d'atténuation peuvent être prises) et une fois qu'un correctif est disponible. Enfin, elle est éliminée une fois le correctif déployé dans le système des utilisateurs.

À cette notion de variation du risque avec le cycle de vie de la vulnérabilité s'ajoute le fait que les parties prenantes ont des appétences différentes au risque. Ceci est vrai aussi bien pour le chercheur en sécurité que pour le responsable du système d'information affecté. *Quid* d'une divulgation laissant une fenêtre temporelle considérable entre la découverte et le signalement ? Et qu'en est-il si l'intermédiation est assurée par des acteurs aux motivations politiques ou financières floues ?

Il est donc primordial de maîtriser, autant que faire se peut, le chaînon fondamental de la divulgation, afin de garantir la connaissance restreinte de l'existence et l'impact potentiel de la vulnérabilité. Selon les acteurs concernés, les questions posées sont distinctes. Les États prendront en compte leurs intérêts nationaux, l'appareil étatique permettant *a priori* une gestion de la divulgation, là où en présence d'acteurs privés, il faut pouvoir garantir une approche et des échanges sécurisés entre l'ensemble des parties prenantes.

II/2 Les outils pour une divulgation coordonnée efficace

Différents moyens existent pour favoriser l'implémentation d'une approche pertinente de divulgation coordonnée de vulnérabilités. Le « premier contact », soit l'établissement d'une conversation entre le chercheur en sécurité ayant découvert une vulnérabilité et le responsable du système d'information affecté, est le point névralgique d'une CVD. C'est pourquoi nous explorons ci-dessous les principaux moyens d'établir ce lien.

II/2.1 Une politique de divulgation *via* un CERT

Une organisation accueille un CERT, ou fait appel à un tel service par le biais d'une société de services managés. Il est alors possible de diriger toute divulgation de vulnérabilités vers le CERT, qui assurera la coordination des parties prenantes, intervenant en tant que conseil, intermédiaire et communiquant. De même, les CERT sont les mieux placés pour préserver une nécessaire discrétion pré-divulgation. En effet, il laisse aux équipes le temps de corriger mais il assure également une vigilance quant aux actifs concernés afin de garantir que la vulnérabilité n'a pas été redécouverte et exploitée entre-temps.

Dans une projection plus systémique, on imagine facilement la nécessité d'avertir les opérateurs les plus essentiels, qui seraient concernés par un risque mais aussi certains services de l'État indispensables pour la survie de la Nation. Ainsi, la prise en charge par un CERT permet d'assurer la diffusion d'une telle information à des tiers concernés de façon privilégiée et rapide. Le cercle de communication peut être modulé avant que le correctif ne soit diffusé à l'ensemble des utilisateurs. Il évite ainsi toute utilisation malveillante. Le CERT-EU, par exemple, permet de telles interactions entre les différents CERT nationaux.

II/2.2 Indiquer les canaux de communication *via* `security.txt`

Face à la difficulté d'identifier un point d'entrée, permettant la remontée de vulnérabilités, des experts de la communauté de cybersécurité ont proposé un standard : un fichier nommé **`security.txt`**, localisé à un endroit connu à l'arborescence de chaque site web. La localisation connue et devant être respectée est la suivante : **`www.monsiteweb.tld/.well-known/security.txt`**.

Différentes organisations, telles que BlaBlaCar, Facebook ou Google, ont déjà adopté ce canal de communication et ce, malgré le caractère non officiel de ce standard. En effet, le projet est soumis à l'IETF (*Internet Engineering Task Force*, un groupe de travail international qui participe à l'élaboration des standards Internet) pour examen et une éventuelle adoption en tant que standard.

II/2.3 Soumettre un rapport *via* ZeroDisclo.com

ZeroDisclo.com est une plateforme, opérée par YesWeHack, qui permet de signaler des vulnérabilités tout en gardant l'anonymat. Grâce à ZeroDisclo, la divulgation peut également se faire *via* le navigateur Tor. Le rapport est chiffré avec la clé publique de l'organisation réceptrice, puis signé et horodaté par une *blockchain*. Le site envoie le rapport (à un CERT privé ou national, par exemple) et le chercheur signalant la vulnérabilité reçoit un certificat en guise de preuve de dépôt.

Cette plateforme propose un parcours de divulgation intéressant. En effet, elle formalise le rapport par le biais notamment de différents critères permettant le calcul du score de sévérité CVSS. Plus important encore, grâce au chiffrement du rapport avec les clés de la personne qui soumet le rapport et le CERT destinataire, ZeroDisclo fait office de « courroie de transmission ». À aucun moment, la plateforme ou les individus qui l'administrent n'accèdent aux détails de la vulnérabilité décrite.

Ce fonctionnement permet de faciliter la divulgation coordonnée de vulnérabilités, sans que ZeroDisclo n'ait à engranger une connaissance dangereuse des défaillances affectant les systèmes d'information de tiers. Ce fonctionnement respectueux contraste avec les pratiques de certaines plateformes de *Bug Bounty* américaines, proposant de recevoir le rapport de vulnérabilités pour une organisation, sans que celle-ci ait donné son accord, et sans aucune transparence quant au véritable devenir de la défaillance signalée (délais de notification aux concernés, réception en clair, stockage… ?).

LE NÉCESSAIRE PARTAGE SOUS CONTRÔLE DE VULNÉRABILITÉS *0DAY*

Des initiatives telles que *ZeroDay Inative (ZDI)* ou encore Google Project Zero ont vu le jour afin de canaliser le partage de vulnérabilités. Se concentrant sur un type particulier de vulnérabilités, à savoir les *0day*, ZDI propose aux personnes qui ont découvert des vulnérabilités la possibilité de divulguer tout en ayant l'assurance que ZDI ne revend, ni ne redistribue, ces défaillances. En effet, ZDI agit en tant qu'intermédiaire avec l'éditeur du service concerné en lui communiquant la vulnérabilité identifiée de manière responsable. Si, à l'issue d'un délai de 120 jours, l'éditeur n'a pas agi, ZDI communique publiquement certains éléments sur la vulnérabilité dont des détails de correction. Le délai pratiqué par Google Project Zero est de 90 jours.

Ces initiatives agissent donc de façon radicalement différente de Zerodium et autres sociétés privées, plus ou moins clairement identifiées comme revendeurs de vulnérabilités *0day*. Zerodium, la plus connue, publie sur son site une grille de rétribution en fonction de la nature des vulnérabilités, allant jusqu'à plusieurs millions de dollars par défaillance identifiée. Une coopération internationale entre professionnels du numérique existe : il est possible de s'en inspirer pour renforcer la gestion des *0day*. Développer un procédé coopératif, à la fois au stade de la recherche, de la communication et du correctif, soutenu par un modèle économique et institutionnel dédié, est la seule façon d'assécher le nombre de vulnérabilités disponibles pour mener des actions malveillantes.

II/**3** Le *Bug Bounty*, une approche complète de divulgation coordonnée de vulnérabilités

Le *Bug Bounty*, aussi appelé « sécurité crowdsourcée », est une manière collective d'éprouver la sécurité d'un produit ou d'un service. Chaque vulnérabilité identifiée est récompensée par le responsable du système concerné, en fonction de sa sévérité et donc du risque que sa correction subséquente permet de réduire. Dans sa déclinaison actuelle, une plateforme de *Bug Bounty* rassemble des chercheurs éthiques internationaux et regroupe différents programmes qui peuvent être publics et privés.

Un programme de *Bug Bounty* soumet un service numérique (site web, API, application mobile, etc.) ou un produit (une voiture connectée par exemple) à des hackers éthiques afin de leur permettre d'y chercher des vulnérabilités potentielles. Dans le cas des programmes publics, tout hacker éthique inscrit sur la plateforme, peut participer. Si le programme est privé, seul un groupe de hackers présélectionnés y prend part.

Le *Bug Bounty* émerge comme un futur standard de la cybersécurité en ce qu'il matérialise la responsabilité collective en matière de réduction du risque numérique. En effet, le *Bug Bounty* incarne la transition (quelque part à l'encontre de la sagesse populaire) du contrôle centralisé de la sécurité de l'information vers une approche « décentralisée », cristallisée par l'implication d'une communauté de hackers éthiques. Cette sécurisation par le collectif est aussi une façon de réduire la quantité de vulnérabilités susceptibles d'être vendues à des intermédiaires aux motivations floues, voire malhonnêtes. En effet, le chercheur rapportant la vulnérabilité reçoit une récompense financière et nourrit son capital social.

On voit un réel engouement pour le développement de cette activité qui vise à préempter toute exploitation malveillante des vulnérabilités, et participe au développement du hacking éthique. Les États et les administrations y ont également recours, à l'image du programme *Hack the Pentagon* de 2016 et de l'annonce en ce sens du ministère des Armées en janvier 2019 grâce à YesWeHack.

Ces plateformes permettent la coordination entre une organisation (institution publique, entreprise privée ou encore association à but non lucratif) qui désire éprouver la sécurité de ses systèmes, et une communauté de chercheurs éthiques qui reçoivent reconnaissance et compensation du fait de leurs découvertes. Les chiffres indiquent la croissance exponentielle de ce marché. Il contribue notamment à une meilleure prise en compte de ce risque, notamment en matière économique.

La réduction globale et durable du risque passera donc par la coopération d'acteurs publics et privés. Un modèle international en la matière est indispensable afin d'éviter toute divulgation publique non coordonnée. Ainsi, garantir une protection à ces chercheurs est déterminant. La question du partage d'information est donc cruciale, et les acteurs privés jouent un rôle important à ce stade. En ce sens, le plugin *YesWeHack VDP Finder* pour Chrome et Firefox permet de savoir si un site web que l'on visite a une politique de CVD existante, qu'elle soit déclinée *via* un e-mail à un CERT, un `security.txt` ou un *Bug Bounty*.

QU'EST-CE QU'UNE POLITIQUE DE DIVULGATION COORDONNÉE ?

Une politique de divulgation de vulnérabilité (*Vulnerability Disclosure Policy* ou VDP), parfois surnommée politique de divulgation responsable (*Responsible Disclosure Policy* ou RDP), décrit comment l'organisation traitera les rapports de vulnérabilités soumis par des hackers éthiques. Il s'agit d'une déclaration ayant valeur juridique. En publiant une VDP, une organisation établit des règles que les chercheurs en sécurité découvrant des vulnérabilités sur les actifs numériques de l'organisation doivent respecter ; si tel est le cas, l'organisation s'engage *a minima* à ne pas les poursuivre.

Une VDP contient en général les éléments essentiels suivants :

/ une déclaration d'engagement en faveur d'une meilleure sécurité de service et des données des utilisateurs. Ce message s'adresse non seulement aux hackers éthiques, mais aussi aux clients, aux médias et aux partenaires potentiels ;

/ une clarté juridique pour les chercheurs en sécurité qui identifieraient des défaillances. Cet élément permet d'instaurer la confiance entre le hacker éthique et l'organisation concernée ;

/ un périmètre afin d'identifier clairement les actifs couverts par la politique de divulgation de vulnérabilités. C'est également une bonne idée de répertorier une section « hors champ », car une organisation peut ne pas vouloir recevoir de rapports de défaillances sur les anciennes versions de services qu'elle ne prend plus en charge. En plus de répertorier les actifs qui entrent dans le champ d'application, il est pertinent d'identifier les types de vulnérabilités qui méritent d'être signalées. En effet, toutes les vulnérabilités ne causent pas réellement de dommages, voire, l'organisation peut déjà les connaître ;

/ le mécanisme de soumission d'un rapport de vulnérabilités et son contenu (détails techniques, format, etc.). Ce volet est essentiel car il précise le moyen d'établir le « premier contact » et rend la communication entre le hacker éthique et l'organisation receveuse en plus aussi facile que possible.

L'objectif de l'ensemble des règles spécifiées dans une VDP est de définir des directives opérationnelles et de communication claires afin qu'elles soient bénéfiques aux parties prenantes. Ces directives sont déclinées en processus de divulgation coordonnée de vulnérabilités, précisant les rôles et responsabilités de toutes les fonctions impliquées et les délais de réaction.

Une VDP doit donc être facilement identifiable *via* un moteur de recherche et accessible sur le site web de l'organisation. Une façon simple pour ce faire est d'utiliser une notice `security.txt` ou un emplacement indiqué par une URL non ambiguë, telle que www.monsiteweb.tld/politique-divulgation-vulnerabilites. Une VDP peut également se matérialiser *via* un *Bug Bounty*, comme est par exemple le cas de BlaBlaCar. Dans ce cas, le programme de *Bug Bounty* est la politique de divulgation de vulnérabilités prévoyant des récompenses financières pour les hackers éthiques.

Mobiliser l'intelligence collective pour mieux (se) protéger

1 Le CERT pour prévenir, réagir, relayer

1/ Il peut assurer la coordination des parties prenantes, conseiller et préserver la discrétion pré-divulgation.

2/ Il veille à la redécouverte et l'exploitation par des acteurs malveillants de la vulnérabilité signalée.

2 Security.txt, le « premier contact » en mode texte

1/ Il offre une porte d'entrée, facilement accessible, aux hackers éthiques.

2/ Ce canal de communication, entre le chercheur en sécurité et l'organisation concernée, permet une remontée efficiente de vulnérabilités.

3 ZeroDisclo.com, une plateforme simple mais efficace

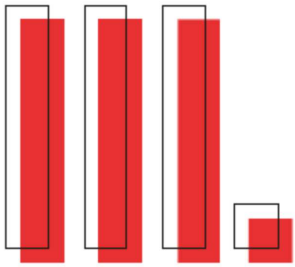
1/ Elle préserve l'anonymat de la personne qui révèle la vulnérabilité tout en assurant un suivi via la signature et l'horodatage immuables d'une *blockchain*.

2/ Le parcours de divulgation de la vulnérabilité est chiffré afin de garantir la confidentialité et l'intégrité des informations.

4 Le *Bug Bounty*, l'approche la plus complète

1/ Le *Bug Bounty* crée une véritable collaboration entre une communauté de hackers éthiques et l'organisation souhaitant éprouver la sécurité de ses systèmes.

2/ Fédérer des chercheurs de vulnérabilités, à travers la reconnaissance, réduit le détournement des failles à des fins malhonnêtes. Il crée également une dynamique vertueuse de réduction des risques.



INNOVEZ, VOUS ÊTES PROTÉGÉS : LA CVD GARANTIT UN CYBERESPACE PLUS SÛR

La divulgation coordonnée de vulnérabilités gagnerait à être promue plus fortement partout en Europe. Cela doit notamment passer par une politique de protection à l'égard des chercheurs en sécurité pour les encourager à utiliser les mécanismes de divulgation coordonnée de vulnérabilités. De même, afin de fluidifier les contributions de ces hackers éthiques, il convient de stimuler la mise en place de politiques de divulgation par les organisations opérant sur le territoire européen.

Dans ce livre blanc, nous avons identifié trois grands obstacles à la participation d'un chercheur en sécurité dans un processus de divulgation de vulnérabilité :

/ les obstacles juridiques ou l'incertitude juridique ;

/ la méconnaissance de moyens appropriés de divulgation de vulnérabilités ;

/ une communication avec le responsable du système ou le coordinateur insuffisante ou trop lente.

Il est donc essentiel de créer un environnement juridique et organisationnel dans lequel le chercheur en sécurité se sente suffisamment protégé et en confiance pour signaler une vulnérabilité au responsable du système d'information concerné qui en assurerait la correction rapide.

À ce jour, seuls certains États membres de l'UE envisagent la création d'une politique nationale coordonnée de divulgation de la vulnérabilité. Deux pays ont déjà mis en place une politique en matière de droits compensateurs, mais les autres États membres n'ont pas de plan immédiat dans ce domaine. Un obstacle important, à la mise en œuvre des politiques en matière de droits compensateurs dans l'UE, est l'absence d'une interprétation unique parmi les États membres de ce qui constitue un « piratage ».

Par conséquent, la première étape consiste à fournir la sécurité juridique nécessaire aux chercheurs en sécurité impliqués dans la découverte de vulnérabilités. Ainsi, il est essentiel de mettre en place des processus appropriés de divulgation des vulnérabilités à travers des conseils complémentaires et de meilleures pratiques.

À cette fin, nous formulons des propositions d'action législative au niveau national et européen. En outre, comme nous l'avons vu plus haut, l'approche législative n'est pas la seule permettant une procédure efficace de CVD. Ainsi, nous suggérons des actions de gouvernance et d'outillage qui créent un environnement vertueux favorisant la collaboration et réduisant durablement le risque numérique.

III/1 Amélioration par le législateur national

Les États membres devraient agir en créant la sécurité juridique nécessaire pour les chercheurs en sécurité impliqués dans la découverte de vulnérabilités par le biais d'une révision de la législation nationale. Elle permettrait la reconnaissance du hacking éthique et offrirait une clarté juridique nécessaire pour les chercheurs en sécurité. En France, plusieurs pistes sont possibles permettant de fluidifier les interactions constructives entre les hackers éthiques et les responsables de système d'information concerné.

Afin d'assurer une meilleure protection des hackers éthiques, une révision du Code pénal est nécessaire. Celle-ci introduira les conditions de protection des chercheurs en sécurité de bonne foi d'éventuelles poursuites judiciaires engagées par l'éditeur de logiciel concerné, son sous-traitant et ses exploitants. De même, la loi Informatique et Libertés dans sa version de juin 2018 pourrait être amendée pour inclure les modalités de protection des chercheurs éthiques.

Afin de consolider la prise de conscience des enjeux d'identification et de correction de vulnérabilités, la loi pourrait obliger les entreprises à afficher sur leur site Internet la démarche à mobiliser en cas de découverte d'une vulnérabilité. Cette obligation pourrait, dans un premier temps, concerner les opérateurs d'importance vitale (définis par la Loi de programmation militaire), les opérateurs de services essentiels et les fournisseurs de services numériques (définis par la Directive européenne NIS transposée en France en 2018).

III/2 Harmonisation au niveau européen

Ce cadre européen, tout juste émergeant et incomplet en matière de divulgation coordonnée de vulnérabilités, n'a pour l'instant pas permis une harmonisation des législations et/ou des pratiques au sein de l'Union européenne. En effet, les politiques européennes s'adressent essentiellement aux organisations publiques ou privées, mais pas aux États membres eux-mêmes. L'absence de politique européenne forte, en matière de protection des chercheurs de bonne foi et de divulgation coordonnée de vulnérabilités, s'accompagne logiquement d'un paysage européen très fragmenté.

Cependant, force est de constater que l'Union européenne se saisit progressivement du sujet de la CVD, comme le montre l'inclusion d'exigences relatives à la divulgation de vulnérabilités dans le *Cybersecurity Act*. Sa mise en œuvre concrète apportera des éléments de réponse quant à l'impact réel du texte sur la divulgation coordonnée de vulnérabilités. Le futur Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité pourrait également financer des projets visant à améliorer les pratiques en matière de divulgation coordonnée de vulnérabilités en Europe.

Une harmonisation *a minima* de la législation européenne est nécessaire afin de réduire de façon significative l'incertitude légale à laquelle sont confrontés bon nombre de chercheurs en sécurité, surtout dans des situations transfrontalières. Afin de renforcer et consolider les efforts en faveur de règles et procédures communes entre les États membres permettant un processus partagé de divulgation coordonnée des vulnérabilités logicielles en Europe, l'UE pourrait notamment :

- **amender la Directive Cybercrime** (Directive 2013/40/EU sur les attaques contre les systèmes d'information), afin d'intégrer la divulgation coordonnée de vulnérabilités, de promouvoir la protection des chercheurs en sécurité et de les encourager à participer à des programmes de divulgation de vulnérabilités. L'article 3 de la Directive pourrait ainsi être amendé afin que les États membres prennent en compte le cas spécifique des hackers bien intentionnés dans leur législation nationale. Une telle harmonisation minimale fournirait une protection accrue aux hackers, tout particulièrement dans les situations transfrontalières ;

/ **inciter les États membres à mettre en place des politiques qui encouragent les entités privées et publiques à établir leur propre politique de divulgation coordonnée des vulnérabilités,** à l'instar des Pays-Bas. Les États membres devraient veiller à ce que les hackers bien intentionnés n'encourent pas de poursuites pénales s'ils prennent part à une divulgation coordonnée de vulnérabilités. Ainsi, une politique européenne globale viendrait compléter concrètement les amendements de la Directive Cybercrime et assurerait que les États membres préservent l'esprit du texte en adaptant leurs législations nationales ;

/ **favoriser un processus harmonisé et équitable de CVD inter-gouvernemental en Europe.** Les gouvernements peuvent être amenés à acquérir des informations sur les vulnérabilités logicielles. L'adoption de politiques rigoureuses pour examiner et coordonner la divulgation des vulnérabilités au niveau des gouvernements et leurs agences devrait être facilitée au sein de l'UE. Pour remédier à l'insuffisance de l'effort, nous recommandons que les États membres adoptent des politiques et des pratiques conçues pour partager des informations. Ces activités devraient être soumises à un contrôle indépendant et impliquer tous les ministères concernés. Le secrétariat exécutif ou, plus généralement, l'organe de coordination de cet effort devrait être hébergé dans une agence civile avec une expertise dans la divulgation coordonnée des vulnérabilités, et fonctionner selon une politique par défaut de divulgation immédiate à(aux) éditeur(s) concerné(s) afin de permettre la correction rapide de toute vulnérabilité ;

/ **prioriser, par le biais de l'ENISA, la ré-édition d'un guide avec la ligne de bonne conduite à adopter.** Il répondrait aux questions soulevées dans l'édition 2015 ;

/ **mettre en œuvre une formation spécifique** dédiée à toutes les questions qui peuvent se poser dans le contexte de la divulgation coordonnée de vulnérabilités, que ce soit au niveau technique ou au niveau juridique.

III/3 Gouvernance de la sécurité et CVD

Les exemples décrits dans ce livre blanc nous montrent qu'un système décentralisé, employant des outils dédiés, permet de mettre en place une politique de divulgation coordonnée de vulnérabilités sans légiférer et ainsi de créer un écosystème à même d'atteindre ces objectifs. Le *Bug Bounty*, notamment, favorise la divulgation coordonnée de vulnérabilités, tout en assurant une protection et une récompense pour les chercheurs en sécurité.

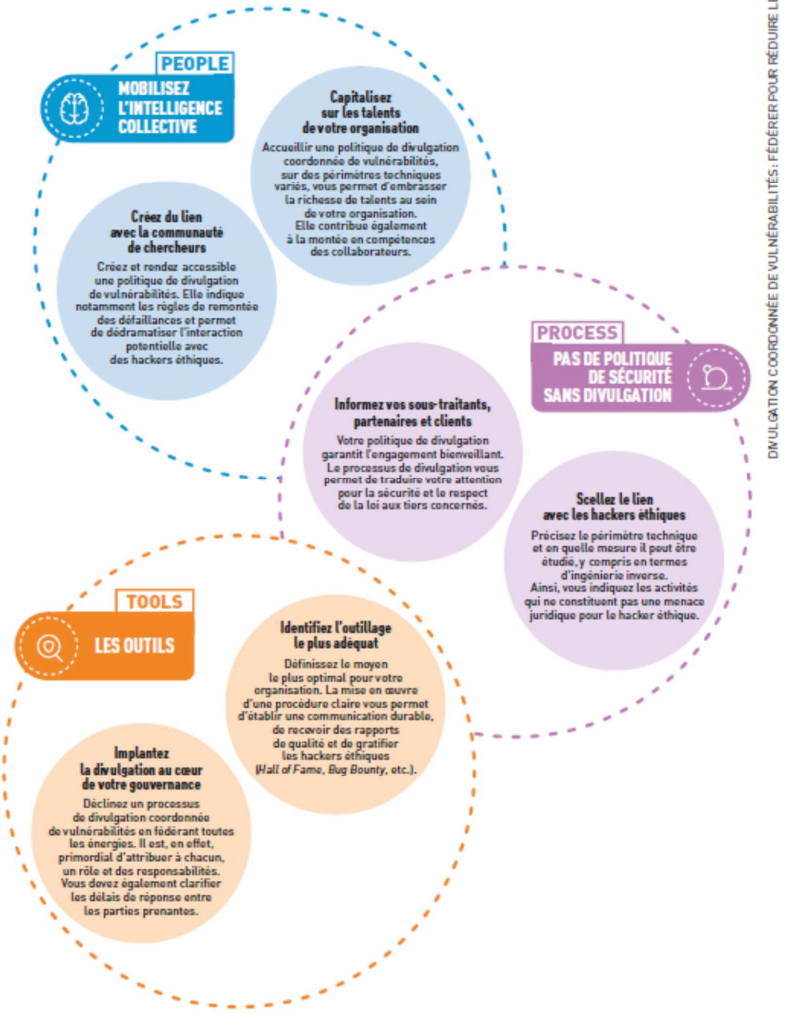
Des alternatives non législatives existent également, reposant sur le triptyque *people – process – tools* (l'humain, les procédures, les outils). Il s'agit de la structuration d'approche holistique prenant en compte :

- **la nécessité de former les personnes impliquées,** notamment les équipes en charge de traiter les remontées de vulnérabilités (réception, triage, qualification, cascade vers les responsables des actifs pour correction, etc.) ;
- **la présence de procédures claires, connues et tenues à jour** de divulgation de vulnérabilités : information de contact, délais de réponse, etc. L'existence d'une politique de CVD – dont ces procédures sont la déclinaison opérationnelle – doit être publicisée de façon appropriée, visible et en termes non ambigus ;
- **l'outillage adéquat de mise en musique de procédures et d'actions,** tel qu'un canal de communication sécurisé (e-mail, programme de *Bug Bounty* privé ou public, page `security.txt`, etc.).

Chaque volet de ce triptyque peut naturellement être décliné en fonction de la profession concernée. Ainsi, la montée en compétences, nécessaire des personnes impliquées (axe *people*), doit également concerner les magistrats. Les personnels du système judiciaire devraient être formés et/ou recevoir des lignes directrices claires et concrètes afin de pouvoir déterminer s'ils sont face à un cas de hacking éthique. Ces initiatives pourraient être mises en place tant au niveau national qu'européen.

Ainsi, le secteur privé a un rôle de chef de file à jouer dans la mise en œuvre de processus de divulgation coordonnée des vulnérabilités. Il peut notamment définir et publier, sur les sites web des entreprises, des mécanismes de rapports publics sur la divulgation des vulnérabilités inspirés des normes ISO. Les équipes de CERT commerciaux et internes aux entreprises peuvent également contribuer à instaurer un cadre collaboratif pour la mise en œuvre des processus de CVD en jouant le rôle de tiers de confiance ou encore de centre de coordination.

« Savoir pour prévoir, afin de pouvoir » : pense-bête pour décideur pressé



RÉFÉRENCES

/ Guide on vulnerability disclosure, ENISA, 2015 : https://www.enisa.europa.eu/publications/vulnerability-disclosure

/ ISO/IEC 29147, ISO/IEC 30111.

/ The CERT Guide to Coordinated Vulnerability Disclosure, Allen D. Householder *et al.*, Software Engineering Institute, Carnegie Mellon University, 2017 : https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

/ Loi pour une République Numérique, 2016 : https://www.legifrance.gouv.fr/eli/loi/2016/10/7/2016-1321/jo/article_47

/ Alerter à propos d'une vulnérabilité, ANSSI :
https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/

/ « Amendement Bluetouff » : http://www.assemblee-nationale.fr/14/amendements/3399/AN/271.asp

/ Arrêt dit « Bluetouff » : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000030635061& fastReqId=2077391977&fastPos=8

/ Lignes directrices relatives à la politique de divulgation de vulnérabilités, Nationaal Cyber Security Centrum, Pays-Bas :
https://english.ncsc.nl/get-to-work/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline

/ Openbaar Ministerie. 2013a. 'Beleid OM 'ethische hackers' in lijn met 'leidraad Responsible Disclosure' :
https://www.om.nl/actueel/nieuwsberichten/1832028/beleid-ethische/

/ Software Vulnerability Disclosure in Europe, CEPS, 2018.

/ Protecting Security Researchers' Rights in the Americas, EFF, 2018 : https://www.eff.org/coders-rights-americas

/ Improving Vulnerability Disclosure Together, CISA, 2019 :
https://www.cisa.gov/blog/2019/11/27/improving-vulnerability-disclosure-together

/ Improving Vulnerability Identification, Management, and Remediation, Office of the Federal CIO, USA, 2019 :
https://policy.cio.gov/vdp-draft/

/ Cybersecurity Act :
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.FRA&toc=OJ:L:2019:151:TOC

/ SPARTA : https://www.sparta.eu/

/ Lignes directrices pour une divulgation coordonnée de vulnérabilités au Japon : https://www.ipa.go.jp/files/000044732.pdf

/ The Dragon Is Winning: U.S. Lags Behind Chinese Vulnerability Reporting, Recorded Future, 2017 :
https://www.recordedfuture.com/chinese-vulnerability-reporting/

/ Vulnerability Disclosure Attitudes and Actions, NTIA, 2016 :
http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

/ Data protection bill amended to protect security researches, The Guardian, 2018 : https://www.theguardian.com/technology/2018/jan/09/data-protection-bill-amended-to-protect-security-researchers

/ Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims, WIRED, 2009 :
http://www.wired.com/2009/12/netflix-privacy-lawsuit/

/ 'Anonymous' browsing data can be easily exposed, researchers reveal, The Guardian, 2017 :
https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers

/ Les violations de données personnelles, CNIL, 2018 : https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

/ CERT-EU Responsible Disclosure Policy :
https://cert.europa.eu/cert/newsletter/en/latest_HallOfFame_.html#CERTpolicy

/ Site officiel `security.txt` : https://securitytxt.org/

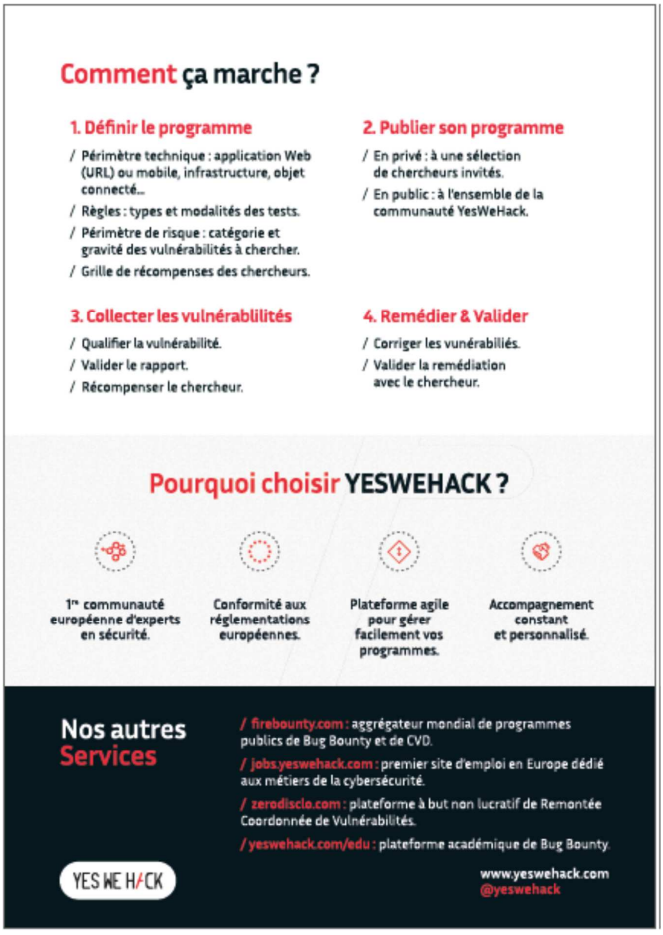
/ https://tools.ietf.org/html/draft-foudil-securitytxt-08

/ Plateforme ZeroDisclo.com : https://zerodisclo.com/

/ Disclosure Policy, ZeroDay Initiative : https://www.zerodayinitiative.com/advisories/disclosure_policy/

/ Adoption de la directive NIS : l'ANSSI, pilote de la transformation en France : https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Livre blanc YesWeHack
Rédaction : YesWeHack - www.yeswehack.com / Janvier 2020.
Conception-réalisation : www.kazoar.fr / Illustrations : Kazoar, Freepik.


Comment ça marche ?
1. Définir le programme
/ Périmètre technique : application Web (URL) ou mobile, infrastructure, objet connecté...
/ Règles : types et modalités des tests.
/ Périmètre de risque : catégorie et gravité des vulnérabilités à chercher.
/ Grille de récompenses des chercheurs.
2. Publier son programme
/ En privé : à une sélection de chercheurs invités.
/ En public : à l'ensemble de la communauté YesWeHack.
3. Collecter les vulnérablilités
/ Qualifier la vulnérabilité.
/ Valider le rapport.
/ Récompenser le chercheur.
4. Remédier & Valider
/ Corriger les vunérabilliés.
/ Valider la remédiation avec le chercheur.
Pourquoi choisir YESWEHACK ?
1re communauté européenne d'experts en sécurité.
Conformité aux réglementations européennes.
Plateforme agile pour gérer facilement vos programmes.
Accompagnement constant et personnalisé.
Nos autres Services
/ firebounty.com : aggrégateur mondial de programmes publics de Bug Bounty et de CVD.
/ jobs.yeswehack.com : premier site d'emploi en Europe dédié aux métiers de la cybersécurité.
/ zerodisclo.com : plateforme à but non lucratif de Remontée Coordonnée de Vulnérabilités.
/ yeswehack.com/edu : plateforme académique de Bug Bounty.
YES WE HACK
www.yeswehack.com
@yeswehack

/ **Ce livre blanc s'appuie sur l'expérience du principal acteur européen de la gestion de divulgation de vulnérabilités, YesWeHack.** Notre ambition est de contribuer à l'élaboration d'un cyberespace moins vulnérable et plus sûr, impulsé par l'Europe. Cette volonté est d'autant plus importante que le risque de cyberattaques, lié à l'exploitation des vulnérabilités, augmentera inévitablement avec la transformation numérique.

/ **Ce livre blanc propose, dans le cadre de la mise en place d'une politique de divulgation coordonnée de vulnérabilités (CVD), des mesures législatives et des recommandations concrètes pour toutes les parties prenantes.** Cette démarche volontaire consolide l'autonomie technologique des organisations et participe au renforcement de la sécurité en Europe. L'organisation responsable et digne de confiance doit ainsi s'attacher à réduire le risque numérique en valorisant les retours de hackers éthiques. C'est cette nouvelle collaboration qui permettra l'émergence d'une responsabilité de cybersécurité collective.

YES WE HACK

Lettre du Club informatique des grandes entreprises françaises (CIGREF) à M. Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance

Cigref
RÉUSSIR
LE NUMÉRIQUE

Paris, le 26 janvier 2021
Réf. 21.003

Monsieur Bruno Le Maire
Ministre de l'Économie, des Finances et de la Relance
139 rue de Bercy
75572 Paris cedex 12

Objet : Cloud de confiance

Référence :

- Lettre du Cigref n° 19.013 du 17 octobre 2019
- Lettre du Cigref n° 20.002 du 17 juin 2020

Monsieur le Ministre,

Dans le contexte actuel, marqué par l'augmentation extrêmement préoccupante de la cybercriminalité, l'accroissement des risques juridiques liés aux réglementations extraterritoriales, notamment américaines, et les incertitudes géopolitiques renforcées par le duel économique et technologique sino-américain, les ambitions nouvelles de la France et de l'Union européenne en matière de souveraineté numérique sont accueillies avec beaucoup d'intérêt par les adhérents de notre association. Cependant, de nombreuses interrogations subsistent sur les actions envisagées par le Gouvernement pour accompagner en France, et à l'échelle européenne, le développement d'une offre de cloud de confiance, en cohérence avec les attentes des grandes entreprises et administrations publiques.

Nous avons eu l'honneur de vous adresser, Monsieur le Ministre, deux courriers, le 17 octobre 2019 et le 17 juin 2020, faisant état des préoccupations de nos adhérents sur ce sujet du cloud de confiance. Nous vous faisions part de nos propositions pour faire converger les besoins de l'Etat en la matière avec ceux des entreprises, lesquelles ne trouvent pas, sur le marché du cloud, les services de confiance, industrialisés et à l'état de l'art, dont elles auraient besoin pour garantir la protection, tant technique que juridique, de leur patrimoine informationnel sensible, tout en disposant des niveau et richesse de services indispensables à leur performance et leur compétitivité. Nous estimons nécessaire, Monsieur le Ministre, d'appeler à nouveau votre attention, par ce courrier, sur plusieurs éléments d'appréciation de la situation. Ces éléments sont le fruit d'une mission d'étude que le Cigref a menée avec l'appui de la société Wavestone dans le cadre de notre groupe de travail sur le cloud de confiance. Cette étude a été réalisée à partir d'un

21 avenue de Messine, 75008 Paris | Tél. : + 33 1 56 59 70 00 | Courriel : cigref@cigref.fr | www.cigref.fr

travail d'enquête et d'interviews d'un groupe représentatif de nos adhérents. Nous tenons à votre disposition les conclusions de cette étude qui mettent en exergue plusieurs facteurs déterminants dont les cinq principaux sont les suivants.

Premier facteur déterminant, nous estimons que la fenêtre d'opportunité qui s'est ouverte, il y a maintenant deux ans, pour faire émerger les offres de cloud de confiance espérées au niveau national, est en train de se refermer en l'absence de signal fort de l'Etat. L'absence de ce signal fort, que nous appelions de nos vœux dans notre précédent courrier, renforce les positions acquises par les offres dominantes de cloud public portées par les *hyperscalers*. A court terme, les entreprises n'auront d'autre choix, compte tenu de leurs échéances contractuelles, des besoins de compétitivité et de services, et des choix technologiques en faveur du cloud des principaux grands éditeurs, que d'arbitrer à nouveau et durablement au profit des *hyperscalers*, réduisant ainsi à une très faible proportion les cas d'usage dont pourrait bénéficier une offre nationale ou européenne de cloud de confiance.

Deuxième facteur déterminant, nous sommes en mesure de vous confirmer le besoin en services de confiance, exprimé par les grandes entreprises membres du Cigref, que nous vous avions transmis dans notre précédent courrier. Cette part de leurs données et des traitements associés que les grandes entreprises pourraient être amenées à confier à un opérateur cloud de confiance apparaît tout à fait significative. Nous estimons, à partir de ce travail d'enquête, que ce marché pourrait se situer, sur le seul périmètre des entreprises adhérentes du Cigref, entre 500 et 800 millions d'Euro, à l'horizon de trois ans, en fonction de la qualité des offres et si celles-ci ne présentaient pas un surcoût de plus de 10% par rapport au marché du cloud public.

Troisième facteur déterminant, les conditions d'émergence d'une offre de cloud de confiance appellent, de notre point de vue, deux conditions essentielles. En premier lieu, un engagement de l'Etat à satisfaire ses besoins propres, au titre du cloud dit dédié et défini dans la stratégie de l'Etat, en étant lui-même primo-client de ces services de confiance, et non uniquement leur financeur. En deuxième lieu, le développement d'une réglementation labellisant des services de confiance et incitant les entreprises, qui recourent à des prestataires de services cloud, à sécuriser leurs données très sensibles et les traitements associés chez des prestataires labellisés. Il est bien entendu qu'une telle réglementation doit accompagner, et non pas précéder, la structuration et la disponibilité sur le marché de telles offres de confiance.

Quatrième facteur déterminant, il ressort de nos consultations que l'échelle européenne est la seule, à terme, à offrir un espace pertinent pour que se développe une offre industrielle et commerciale de cloud de confiance à l'état de l'art et économiquement soutenable. Dans ces conditions, il est indispensable de concevoir les contributions nationales à l'émergence d'une telle offre, dans une perspective européenne, notamment en termes de sécurité et de réglementation. Si l'initiative Gaia-X peut être un inducteur et un facteur de déploiement intéressant pour une telle démarche, elle ne peut être que complémentaire et ne saurait s'y substituer.

Cinquième facteur déterminant, nous avons la conviction qu'il sera nécessaire de s'appuyer sur les technologies des *hyperscalers* pour développer de premières offres de cloud de confiance, à l'état de l'art et au niveau de richesse de services attendu. Nous savons que la plupart d'entre eux y travaillent. Nous

21 avenue de Messine, 75008 Paris | Tél. : + 33 1 56 59 70 00 | Courriel : cigref@cigref.fr | www.cigref.fr

avons conscience qu'une telle stratégie n'est pas dénuée de risques, tant en termes d'image que de dépendance. Des précautions et un suivi particulier de ces initiatives s'avéreront donc indispensables.

Le 7 février 2020, vous aviez reçu, Monsieur le Ministre, une trentaine de représentants de haut niveau de grandes entreprises françaises, pour la plupart directeurs généraux ou directeurs des systèmes d'information de leur groupe, afin d'évaluer avec eux les possibilités qui pouvaient s'offrir pour une action conjointe de l'Etat et des grandes entreprises en matière de cloud de confiance. Nous souhaiterions vous proposer de renouveler ce rendez-vous, à courte échéance. Au cours de cette réunion, nous pourrions, si vous le souhaitiez, vous présenter une synthèse des travaux que nous avons conduits et envisager les perspectives qui restent ouvertes dans les conditions que nous venons de succinctement vous décrire.

A défaut d'une initiative forte de l'Etat en la matière, et d'engagements pris à court terme pour déclencher une dynamique substantielle au profit de l'émergence d'offres de service cloud de confiance, notre association serait conduite à surseoir à ces efforts sur ce sujet, pour consacrer ses ressources à d'autres sujets non moins prioritaires pour nos adhérents.

Monsieur le Ministre, les grandes entreprises françaises expriment des attentes fortes, que l'Etat doit précéder et accompagner pour que celles-ci puissent mutualiser avec lui leurs efforts portés sur le marché du cloud de confiance en France et en Europe. Nous vous renouvelons notre disponibilité pour coopérer avec l'Etat sur ce sujet, lequel sera déterminant pour l'avenir de l'économie de notre continent.

Nous vous prions, Monsieur le Ministre, d'agréer l'expression de notre très haute considération.

Vincent Niebel

Pilote du groupe de travail « Cloud de confiance »
Cigref

Bernard Duverneuil

Président
Cigref

21 avenue de Messine, 75008 Paris | Tél. : + 33 1 56 59 70 00 | Courriel : cigref@cigref.fr | www.cigref.fr

Copie : Madame Florence Parly, Ministre des armées

Madame Amélie de Montchalin, Ministre de la Transformation et de la Fonction publiques

Monsieur Cédric O, Secrétaire d'Etat chargé de la Transition numérique et des Communications électroniques

Monsieur Thomas Courbe, Directeur général des entreprises

Monsieur Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information

Monsieur Nadi Bou Hanna, Directeur interministériel du numérique et du système d'information et de communication de l'État

Monsieur Mohammed Adnène Trojette, Conseiller action publique et numérique, Cabinet du président de la République

21 avenue de Messine, 75008 Paris | Tél. : + 33 1 56 59 70 00 | Courriel : cigref@cigref.fr | www.cigref.fr

AUDITIONS

Rencontre avec Mme Mariya Gabriel, commissaire européenne *(1er octobre 2020)*

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je suis heureux de l'opportunité qui nous est donnée de rencontrer ici, lors de la « Paris Cyber Week », Mme Mariya Gabriel, commissaire européenne chargée de l'innovation, de la recherche, de la culture, de l'éducation et de la jeunesse. Notre mission d'information, qui va durant les prochains mois examiner les voies pour la construction d'une souveraineté numérique, est très attachée à la dimension européenne de celle-ci. À cet égard, nous ne pouvons que nous féliciter de l'accent mis par la présidente de la Commission européenne, Ursula von der Leyen, dans son discours sur l'état de l'Union du 16 septembre, sur l'idée d'une souveraineté numérique européenne comme point de mire de la « décennie numérique » de l'Europe.

Madame la commissaire, vous êtes en charge de secteurs clés pour le futur de l'Union, l'innovation et la recherche, dont la crise liée à la pandémie met aujourd'hui cruellement en lumière le caractère stratégique. Dans votre action de commissaire, quel lien faites-vous entre la promotion du développement de la recherche et de l'innovation d'une part et la construction d'une certaine autonomie européenne d'autre part ? La Commission européenne est-elle assez armée pour tenter d'opérer cette conciliation ? À votre niveau, comment vous appuyez-vous sur l'action effectuée lors de votre précédent mandat, notamment dans le secteur du numérique, pour mener à bien les objectifs assignés par la présidente von der Leyen ?

Au titre de vos attributions, vous êtes très engagée pour l'adoption et la mise en œuvre du programme Horizon Europe dans le cadre du prochain cadre financier pluriannuel. Ce programme cadre pour le futur de la recherche européenne sera-t-il suffisant pour éviter que l'Europe ne prenne du retard dans les secteurs d'avenir (au premier rang desquels le secteur du numérique), alors même que le montant de la proposition initiale de la Commission européenne a été largement revu à la baisse par le Conseil européen de juillet dernier ?

Je laisse la parole à mon collègue, Philippe Latombe, rapporteur de notre mission d'information.

M. Philippe Latombe, Rapporteur. Je souhaiterais d'abord revenir sur l'action de l'Union européenne en matière de recherche pour soutenir le développement des innovations de rupture et des secteurs de pointe du numérique, notamment à travers le programme Horizon Europe. Lors de votre précédent mandat, sous la présidence de Jean-Claude Juncker, vous avez beaucoup contribué au programme Horizon 2020, mais vous avez certainement dû constater des voies d'amélioration. Comment concevez-vous la continuité entre ces deux programmes européens et quels éléments voulez-vous voir développés pour un meilleur soutien à la recherche ? Qu'apportera, selon-vous, l'approche par missions du nouveau programme Horizon Europe et que pouvez-vous nous dire des sommes qui seront allouées dans le cadre du prochain plan financier pluriannuel ? Par ailleurs, votre feuille de route pour la mandature comprend la mise en place d'un Conseil européen de l'innovation. Pourriez-vous nous éclairer sur le rôle de cette nouvelle institution et sur son futur mode de fonctionnement ?

Comment cette initiative va-t-elle s'articuler avec le nouveau programme de financement Digital Europe qui prévoit plus de 8 milliards d'euros dans le prochain programme de financement pluriannuel 2020-2027 pour le soutien au développement de l'intelligence artificielle et de supercalculateurs ? Votre travail sur la mandature précédente a beaucoup contribué à l'élaboration de ce programme, pourriez-vous nous en expliquer les principes ?

L'Europe est souvent présentée comme un terrain privilégié pour la recherche avec de fortes capacités d'innovation, ce dont témoigne par exemple le nombre de brevets déposés rapporté à la population, mais aussi avec une capacité moindre à trouver des applications industrielles susceptibles à la fois de soutenir une croissance durable et d'assurer une certaine autonomie stratégique. Comment l'action de la Commission prévoit-elle de fluidifier les rapports entre recherche fondamentale et applications concrètes ? Quelles sont notamment les pistes pour améliorer le financement des innovations ? Et quels freins avez-vous pu déjà identifier dans la mise en application des résultats de la recherche européenne dans le secteur du numérique ?

Enfin, nous savons que l'Europe souffre de façon croissante d'une perte d'industrie stratégique dans le secteur du matériel informatique qui constitue pourtant le soubassement du développement du numérique. Comment selon vous contrer cette tendance et de quelle façon la Commission entend-elle faire participer l'innovation et la recherche à une certaine forme de réindustrialisation dans ces nouvelles technologies à même d'assurer une plus grande souveraineté européenne ?

Enfin, un dernier point, je souhaiterais vous interroger sur la façon dont vous comptez favoriser la formation et l'éducation. En effet, on nous présente aujourd'hui un nombre trop faible d'experts dans ce domaine, ce qui nuit à ses capacités de développement. L'Europe peine aussi parfois à retenir ceux qu'elle forme. Comment devenir plus efficace en la matière ? De quelle façon la Commission entend-elle de façon plus générale contribuer à mieux former les citoyens à leurs droits et leurs devoirs en matière de numérique ?

Mme Mariya Gabriel, commissaire européenne. L'idéal européen en matière de recherche et d'innovation souffre aujourd'hui d'un manque de cohérence, dans la mesure où, malgré les annonces présentant la recherche et l'innovation comme des éléments essentiels de la résilience et de la relance européenne, le budget originellement prévu a été réduit. De manière surprenante, cette décision ne provient pas des États membres auxquels on aurait immédiatement pensé. Ce sont les pays de l'Est et l'Autriche qui se sont élevés en faveur de l'innovation. Malheureusement, aucun leader n'a appuyé de manière claire le budget du programme Horizon Europe.

Durant les six derniers mois, l'Union européenne a massivement investi dans la recherche et l'innovation. Elle a été particulièrement rapide dans sa réaction à la crise sanitaire puisque les premiers projets de recherche d'un vaccin anti-covid ont débuté le 30 janvier. L'Europe a investi 1,4 milliard d'euros dans la lutte contre l'épidémie. Un milliard provient du programme Horizon Europe. Ont été financés des instituts de recherche, des start-up, des entreprises…

Concernant le budget, l'Union européenne est en pleine période de préparation. Le Conseil a adopté il y a deux jours une position commune pour le programme Horizon Europe. Le budget du programme sera présenté au Parlement la semaine prochaine. Trois chapitres ne sont pas encore finalisés. Le programme doit débuter le 1er janvier 2021.

L'une des questions essentielles dans l'élaboration du programme Horizon Europe est celle des synergies. Cette question est évoquée depuis près de cinq ans mais aucune réunion n'a pour l'instant été organisée entre la direction générale et la direction recherche et innovation à ce sujet. On fait croire aux entreprises européennes que les régions et les États vont pouvoir les financer mais ce n'est pas encore le cas. Comment rassurer nos entreprises ? La question des synergies est prise en compte dans le programme Horizon Europe. Même si le budget alloué à ces dispositions a été réduit, le plan de relance, les fonds de développement régional et les fonds structurels permettront d'améliorer la situation.

Il est essentiel d'avoir un projet Horizon Europe opérationnel au 1er janvier 2021.

Les succès d'Horizon 2020 seront conservés. Horizon Europe continuera de soutenir la recherche fondamentale grâce au Conseil européen de la recherche. Ce conseil est devenu une véritable référence mondiale. Il est donc essentiel de continuer à soutenir nos chercheurs, notamment dans la *frontier research*, la recherche à la frontière de la connaissance.

Les différences avec Horizon 2020 seront importantes dans le deuxième pilier et le troisième pilier d'Horizon Europe. Le deuxième pilier est consacré à la compétitivité, aux partenariats avec l'industrie. Les crédits alloués à ce pilier seront réduits de moitié et orientés vers une nouvelle stratégie. L'approche ne sera plus ici de financer l'activité de manière générale mais de soutenir des projets spécifiques sélectionnés pour leur impact. Le nombre exact de projets soutenus est actuellement débattu. Il y aura très probablement un partenariat dans le domaine de la santé, dans le domaine des technologies de pointe comme l'intelligence artificielle (IA) ou les technologies de communication sans fil de sixième génération (6G). Mais l'important est ici d'évaluer la façon dont ces projets auront le plus d'impact possible. Il faut également éviter que ces partenariats ne se transforment en « clubs » privés. L'ouverture de ces nouveaux partenariats reste une question préoccupante.

La seconde grande nouveauté concerne l'approche par missions. Pour la première fois, un portefeuille d'actions portant sur cinq sujets choisis avec les États membres et le Parlement sera introduit. Les sujets ont été choisis en fonction de leur impact sur la vie quotidienne des citoyens. La première mission est dédiée à la lutte contre le cancer. Les autres missions seront dédiées à la lutte contre le changement climatique, aux eaux, océans et mers, aux villes intelligentes, à la santé des terres et à l'agriculture…

Cela fait plus d'un an que ces missions sont étudiées. Les premiers rapports ont été rendus le 1er juin. Ces rapports ont permis d'identifier des recommandations concrètes qui pourront être mises en œuvre dès l'année prochaine. Le cadre temporel des missions, de 2021 à 2024, est plus limité que le cadre temporel du programme Horizon Europe qui s'étend jusqu'à 2027.

Le Parlement a imposé deux conditions au développement de ces missions : la mesure de leur succès à l'aide d'indicateurs et la limitation de leur financement à 10 % du budget du deuxième pilier d'Horizon Europe.

Les premiers rapports rendus en juin ont été enrichis par l'étude de l'impact de la crise sanitaire et les échanges avec les citoyens européens. Les rapports finaux ont été rendus la semaine dernière. Les objectifs proposés par ces rapports sont particulièrement concrets : 3 millions de vies sauvées d'ici 2030 pour le cancer, 100 villes climatiquement neutres d'ici 2030, 200 régions européennes très avancées sur la neutralité climatique, 75 % de nos terres en bonne santé d'ici 2030… Ces actions doivent maintenant être mises en œuvre de manière opérationnelle.

C'est dans cet objectif d'opérationnalisation que la question des synergies apparaît comme essentielle. Le deuxième pilier du programme Horizon Europe représente aujourd'hui 52 milliards d'euros. La moitié de cette somme sera dédiée aux partenariats et 10 % seront distillés entre les différentes missions. Le budget d'Horizon Europe ne sera pas suffisant. C'est pour cette raison que le soutien des cinq missions se fera par la coopération avec d'autres commissaires européens. Huit commissaires ont été identifiés, comme les transports, l'environnement, la santé, le développement régional...

Un autre enjeu important est la reconnaissance des missions par l'ensemble des citoyens européens. Ces cinq missions sont ambitieuses. Sans cette reconnaissance il sera difficile de les mener à bien.

Le troisième pilier d'Horizon Europe se différencie également d'Horizon 2020 par la création d'un Conseil européen de l'innovation. Son ambition est de soutenir la création de licornes européennes en identifiant les start-up et petites et moyennes entreprises (PME) les plus prometteuses. Les start-up et PME seront directement financées dans leur phase de développement la plus risquée : le passage de la recherche à la commercialisation. Cette phase, incluant le passage du produit au marché et le déploiement industriel et commercial de prototypes, représente 70 % du budget total des start-up et PME. 100 milliards d'euros seront consacrés à ces aides. Le Conseil européen de l'innovation a déjà commencé à fonctionner : 5 000 entreprises ont déjà été soutenues pour un total de 4 milliards d'euros. Un enjeu important dans le développement du Conseil européen de l'innovation tient au soutien des États membres. Ces derniers viennent malheureusement de voter une coupe de son budget de 200 millions d'euros.

L'espace européen de la recherche doit également être redynamisé. L'Europe est toujours à moins de 3 % d'investissement dans la recherche et les chiffres sont encore plus faibles lorsqu'il s'agit d'investissements privés. Il faut prioriser ces investissements. Un cadre commun avec les États membres va être mis en place. Il est nécessaire de travailler à l'accès à l'excellence pour tous. 5,6 % du budget recherche du programme Horizon 2020 est allé vers les *widening countries* (pays de l'élargissement) et 94,6 % aux quinze autres pays. Ce n'est pas normal. Les « clubs » fermés sont à éviter. Une véritable stratégie commence à voir le jour : 3,3 % du budget d'Horizon Europe sera dédié aux *widening countries*. C'est à l'Union européenne de développer de tels mécanismes.

L'Europe doit également lutter contre le problème du *brain drain*, de l'exode des compétences. Nos talents ont besoin de se sentir soutenus. Il faut soutenir leurs idées. Pour la première fois, l'un des objectifs est de traduire rapidement les résultats de la recherche scientifique en innovation. L'Europe est riche en sciences, elle produit 20 % des publications scientifiques dans le monde. L'effort doit porter sur la traduction de cette recherche en innovation. Des feuilles de route technologiques avec le monde académique, la recherche et l'industrie ont été proposées. La coopération avec la stratégie européenne de l'industrie est aussi en cours de développement.

Concernant l'éducation, la formation et les compétences numériques, un plan actualisé de l'éducation numérique et la création d'un espace européen de l'éducation d'ici 2025 ont été proposés. Le premier plan pour l'éducation numérique datait de 2018 et était trop limité dans le temps. Le nouveau plan développe une stratégie de long terme de 2021 à 2027. Le premier plan était focalisé sur l'éducation formelle. Le nouveau plan inclut éducation non formelle et formation professionnelle.

Les leçons de la crise sanitaire ont fait apparaître le problème de la connectivité des zones rurales. Le plan de relance pourrait permettre de travailler sur cette question et de doter les États membres de nouveaux équipements.

La question du contenu en ligne de haute qualité doit également être abordée. Trois plateformes proposent aujourd'hui ce type de contenus, aucun d'entre elles n'est européenne. Ces plateformes totalisent 73 % des utilisateurs de ces contenus en ligne en Europe. Une plateforme européenne pourrait être mise en place. Cette idée peine encore à se faire accepter. Une étude de faisabilité est prévue pour l'année prochaine.

Pour développer l'éducation numérique en Europe, un projet de développement dans chaque État membre de « *Digital Education Hubs* » est en train de voir le jour. Ces lieux centraliseraient les informations sur l'éducation numérique, les compétences et la formation dans ce domaine. Les compétences numériques doivent être séparées entre compétences de base et compétences avancées. Seulement 36 % de la force de travail européenne maîtrise les compétences numériques de base, 44 % des citoyens européens les maîtrisent, tandis que 90 % des offres d'emplois les exigent. Un effort important est nécessaire. Concernant les compétences avancées, l'Europe manque de spécialistes en IA. Elle manque de 300 000 experts en cyber dès aujourd'hui et ce nombre ne cesse d'augmenter. Une augmentation de 70 000 emplois a été signalée récemment. Pour la première fois, grâce au projet Digital Europe, 700 millions d'euros seront dédiés aux compétences numériques avancées. Un accent particulier doit être porté sur l'IA. Cette technologie est le prochain « *game changer* », ce qui va permettre de changer la donne. L'Europe a besoin de spécialistes, de femmes notamment.

Sur la question de l'IA, il est important de développer une approche européenne de cette nouvelle technologie. Cette approche doit inclure des principes éthiques clairs qui permettent de prévenir les discriminations.

Mme Frédérique Dumas. Vous avez évoqué la question de l'association de l'Europe avec le reste du monde. Quels sont les pays concernés ? Une association avec Taïwan, État particulièrement avancé dans le domaine du numérique, est-elle envisagée ? Vous avez également abordé la question de l'opérationnalisation, qu'en est-il réellement ?

Mme Mariya Gabriel, commissaire européenne. Horizon Europe est un programme très ouvert. Le développement de la science ne peut se faire sans échanges internationaux. Notre approche doit être aussi ouverte que possible et aussi fermée que nécessaire. Cette question de l'ouverture du programme aux pays tiers a récemment été intégrée dans les règlements. Horizon Europe se réserve dorénavant le droit de ne pas accepter les entreprises contrôlées par des pays tiers non associés au programme. Cette sélection se fera de manière transparente, au cas par cas, la politique extérieure étant un sujet délicat. Tous les États membres n'entretiennent pas les mêmes relations internationales.

La question de l'association des pays tiers au programme est divisée en quatre catégories. L'association la plus proche et la plus complète concerne seize pays déjà associés au programme Horizon 2020. La question d'ouvrir cette association à des pays ne partageant pas de frontières avec l'Europe mais des valeurs et un même niveau technologique est aujourd'hui engagée avec le Parlement. L'Australie, la Nouvelle-Zélande, le Japon et la Corée du Sud ont demandé à être associés. Taïwan n'a envoyé pour l'instant aucune demande.

Une seconde nouveauté est la possibilité évoquée de ne pas donner à certains pays tiers l'accès à certains piliers du programme Horizon Europe. Ces restrictions concernent principalement le troisième pilier car son budget est restreint et nos entreprises en ont besoin. Les appels à projet du Conseil européen de l'innovation reçoivent de nombreuses propositions. Un pays a remporté 32 % du budget. Trois pays ont reçu 60 % du budget. Quand ces pays ne respectent pas le principe de réciprocité il y a un problème. C'est notamment le cas de la Chine dont le comportement nécessite un changement d'approche de la part de l'Union européenne. Des lignes rouges vont être tracées dans le domaine de la science et de la recherche. Si le principe de réciprocité n'est pas respecté, l'accès au programme se fermera. Les échanges avec les autorités chinoises ont été décevants, ces dernières expliquant qu'il n'y avait qu'un malentendu et que l'Europe avait mal compris leurs lois. Lorsqu'il s'agit de souveraineté et d'autonomie, l'Europe se doit d'être cohérente.

M. Denis Masséglia. Comment expliquer le départ des ingénieurs européens aux États-Unis ? Comment faire progresser et protéger le marché européen du numérique ? Fermer les frontières ? Investir massivement dans la recherche ?

Mme Mariya Gabriel, commissaire européenne. L'Europe est composée de 27 législations, 27 langues, 27 certifications. Les États-Unis ont une seule langue, une unique législation.

Le marché européen du numérique n'existe pas encore. Le déploiement de l'interopérabilité a été décidé il y a deux ans. Rien n'a pour l'instant été mis en place. L'idée d'un portail unique pour les entreprises avait également été abordée mais n'a toujours pas vu le jour. Le règlement sur la responsabilité des plateformes n'a donné aucun résultat. La crise sanitaire a permis de comprendre l'importance du soutien à nos entreprises dans ce secteur afin de les protéger de leur dépendance vis-à-vis d'acteurs étrangers. Je crois en la force des exemples. Il faut que les entreprises sachent que l'Europe les soutiendra. Nous avons deux entreprises qui comptent parmi les cinq meilleures dans le secteur des vaccins. Pour les favoriser par rapport aux offres chinoises et américaines, de grands efforts ont été déployés. On a ainsi découvert pendant la crise que certains mécanismes permettaient de favoriser les entreprises européennes. Il faut développer cette approche. Le soutien ne doit pas nécessairement concerner seulement les entreprises européennes mais également les entreprises étrangères qui choisissent de s'installer en Europe.

Le problème de la temporalité est également majeur. Il est difficile d'expliquer à une start-up qu'elle recevra ses financements dans cinq ou six ans quand elle est à trois ans de la faillite.

Mme Amélia Lakrafi. Concernant le problème du multilinguisme, les frais de traduction des dossiers sont souvent trop importants pour les start-up. Comment remédier à cette situation ?

Mme Mariya Gabriel, commissaire européenne. Un effort doit être fait sur les évaluateurs. J'ai proposé de recruter des experts connaissant la langue, la région et le marché concernés pour les différentes entreprises. Cette proposition a été suivie d'un long silence.

M. Pierre-Alain Raphan. Comment évaluer et assurer l'utilité des projets et missions ? Comment accompagner les très petites entreprises (TPE) vers la maturité digitale ? Je fais la proposition d'un « digiscore », inspiré du « nutriscore ».

Mme Mariya Gabriel, commissaire européenne. Concernant la formation digitale professionnelle, cinquante centres d'excellence pour la formation professionnelle vont être déployés. L'accord du Parlement européen est encore nécessaire.

L'idée du « digiscore » est excellente. La développer dans chaque État membre serait surement très utile.

Concernant la mise en œuvre des missions, elle s'appuie sur de nombreux objectifs de développement durable. La présidente de la Commission européenne est très engagée sur cette question. Pour la première fois, des objectifs de développement durable ont été directement intégrés aux programmes. 84 % du programme Horizon Europe contribue directement à ces objectifs. 35 % du budget Horizon Europe devrait être orienté vers la transition verte. Neuf indicateurs, divisés en trois groupes, seront mobilisés. Ces indicateurs ne seront pas seulement économiques mais également humains.

Audition, ouverte à la presse, de représentants du Comité stratégique de filière Industrie électronique (CSF Industrie électronique) *(8 octobre 2020)*

Présidence de M. Philippe Latombe, rapporteur

M. Philippe Latombe, rapporteur. Permettez-moi tout d'abord d'excuser le président Jean-Luc Warsmann, qui est retenu par ailleurs. Il nous rejoindra au cours des auditions de ce matin.

Je me réjouis de la présence des acteurs de la filière des industries électroniques, qui nous font le plaisir de ces échanges alors que les travaux de la mission d'information débutent. M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique (CSF Industrie électronique), est présent aujourd'hui. Il est également vice-président de la Fédération des industries électriques, électroniques et de communication (FIEEC). Enfin, il est président de l'entreprise STMicroelectronics France. Mme Virginie Hoel est professeure des universités et enseigne au sein de l'institut électronique, microélectronique, nanoélectronique de l'université de Lille. Enfin, M. Guillaume Adam est délégué du CSF Industrie électronique et directeur des affaires européennes et numériques à la FIEEC.

Cette audition du comité stratégique de filière s'inscrit dans le cadre des réflexions que nous souhaitons mener sur la souveraineté numérique dans sa partie *hardware*, à savoir le matériel et l'équipement. C'est donc un plaisir « d'entrer dans le dur » du sujet en votre compagnie, autour des enjeux stratégiques, technologiques et géopolitiques de la filière Industrie électronique.

Il n'existe pas de souveraineté numérique sans souveraineté technologique. La filière électronique en constitue un bon exemple. En effet, elle produit des composants indispensables au fonctionnement physique du numérique et fait l'objet de stratégies offensives de la part des États souhaitant se positionner sur des segments de marchés les plus décisifs au niveau mondial.

J'aimerais vous citer quelques chiffres en guise de courte introduction. En France, le chiffre d'affaires de la filière électronique s'élève à 15 milliards d'euros. D'après nos sources, la filière génère 80 000 emplois directs, 170 000 emplois indirects et 8 000 chercheurs publics. J'aimerais également mentionner les fleurons français dans des domaines de pointe. Nous pouvons citer deux exemples, STMicroelectronics, dont le président est présent parmi nous, et Lacroix Group.

Pour débuter notre échange, je vous propose d'aborder deux sujets. Le premier sujet porte sur l'actualité de votre filière, dans un contexte marqué à la fois par la crise sanitaire et, si je puis dire, par une entrée dans la deuxième partie du cycle 2018-2022. Ce cycle concerne aussi bien le contrat de votre filière avec l'État que le plan Nano 2022. Un bilan d'étape nous serait d'ailleurs particulièrement utile dans la perspective du prochain plan Nano. Le second sujet porte sur la souveraineté numérique en tant que telle et la façon dont votre filière l'appréhende au niveau national et européen. En effet, nous avons pleinement conscience que les choix effectués dans ce domaine engagent sur la longue durée et doivent donc être mûrement réfléchis.

Vos éclairages sur ces enjeux nous seraient d'une aide très précieuse, alors que l'Assemblée nationale étudiera prochainement le plan de relance et le contenu du quatrième programme d'investissements d'avenir (PIA).

M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique. J'évoquerai les grandes perspectives de la filière électronique. Il est important de comprendre que la filière est composée de quatre axes. Notons que le terme « électronique » est assez générique. Ces quatre axes sont : les composants électroniques, c'est-à-dire le *hardware* que vous évoquiez ; les cartes et assemblages électroniques, soit l'axe qui achète les composants, les monte sur les cartes, les soude, les teste et en assure la revente ; le syndicat professionnel de la distribution de vente de composants électroniques ; les logiciels temps réel embarqué, axe représenté au sein de la filière par Embedded France.

Les équipements finaux, tels que les téléphones portables ou les infrastructures télécoms, ne font pas partie des axes de la filière. En revanche, la filière est l'un des fournisseurs de ces équipementiers.

À propos de ces enjeux, un plan a été lancé à travers un projet important d'intérêt européen commun (PIIEC), le premier initialisé en Europe sur la nanoélectronique. Ce PIIEC regroupe quatre États : l'Allemagne, l'Italie, l'Angleterre et la France. En France, il porte le nom de plan Nano 2022, ayant fait l'objet d'une notification auprès de la direction générale de la concurrence en décembre 2018. Ce plan a pour objet de soutenir la recherche, le développement et les premiers déploiements industriels. Ce soutien est le principe du PIIEC, comme en témoigne le PIIEC sur les batteries, lancé récemment. Actuellement, les différents États discutent du lancement d'un PIIEC 2, avec un élargissement des États membres européens, dont le démarrage aurait sans doute lieu à l'horizon 2021.

Sur ce plan, sept chefs de file se distinguent en France. Il s'agit d'entreprises, basées en France, ayant des projets de recherche, de développement et d'innovation dans différents domaines.

Ce programme compte cinq piliers, concernant respectivement : le numérique, les technologies digitales et les technologies faible consommation d'énergie ; l'électronique de puissance ; les capteurs, tels que les microsystèmes électromécaniques (MEMS) permettant de réaliser des mesures (boussole, humidité ou encore hydrométrie) ; les substrats ; les outils de production.

Ce plan constitue un tronc commun aux différents acteurs européens, qu'ils soient français, allemands, italiens ou anglais. Chacun des partenaires coopère sur les différents piliers des programmes.

En France, ce programme est également soutenu avec pour chefs de file Soitec, UMC, Lynred, STMicroelectronics, CEA-Leti ou encore X-FAB. Des développements technologiques sont réalisés dans le cadre de ces programmes, alignés avec les stratégies des entreprises afin de subvenir aux besoins des différents équipementiers.

Au sein de la filière, nous dénombrons cinq axes. Le premier axe concerne l'innovation. Selon le contrat de la filière, nous devons développer les briques technologiques nécessaires aux développements des nouvelles technologies.

Le deuxième axe porte sur l'industrie électronique du futur, soit l'utilisation de l'électronique auprès des petites et moyennes entreprises (PME) et entreprises de taille intermédiaire (ETI) pour disséminer un peu plus l'électronique dans le tissu industriel français.

Le troisième axe est relatif aux compétences et emplois. Cet axe constitue un vrai sujet puisque nous avons besoin d'augmenter l'appétence des jeunes pour ce secteur.

Le quatrième axe concerne l'international. Nous nous interrogeons sur la façon de développer l'international en tenant compte du taux d'exportation global d'environ 60 % dans notre filière. Pour les composants électroniques, l'exportation s'élève à 80 % sur la réalisation du chiffre d'affaires français. Je tiens à préciser que, concernant STMicroelectronics, l'exportation est supérieure à 90 %. Il s'agit du chiffre d'affaires en France sur les usines françaises.

Le cinquième et dernier axe porte sur l'intelligence artificielle embarquée, appelée *Edge Computing*. Vous connaissez sans doute les informations que nous avons sur l'intelligence artificielle dans le *cloud* et l'utilisation des bases de données massives. Une deuxième branche apparaît, pour laquelle nous considérons que la France et l'Europe détiennent une véritable opportunité de prendre le leadership mondial. Cette deuxième branche est relative à la décentralisation de cette intelligence artificielle, afin de traiter ces algorithmes spécifiques près des équipements et non plus dans les serveurs et le *cloud*. Comme vous le savez, le leadership américain est très fort sur les serveurs et le *cloud*.

Nous travaillons dans cette direction, notamment avec les programmes d'accélération sur l'intelligence artificielle actuellement élaborés avec la direction générale des entreprises (DGE), dans le but de pousser l'écosystème français et les coopérations nécessaires, à la fois au niveau du *hardware* (les algorithmes logiciels avec le CEA-List, l'Institut national de recherche en informatique et en automatique [INRIA] ou d'autres organismes) et les acteurs finaux que sont les utilisateurs de l'intelligence artificielle.

Sur le contrat de la filière électronique, nous avons formé sept groupes de travail. Chacun des groupes de travail s'occupe de propositions, soit pour favoriser la recherche, le développement et l'innovation, soit pour travailler sur des coopérations transversales.

La coopération transversale avec les autres filières constitue l'un des grands axes du plan de relance que vous avez précédemment évoqué. Cette coopération est très importante. Nous avons fortement concouru à développer des solutions dans le domaine de la puissance, l'un des piliers du plan Nano 2022. Ce plan nous a permis de coopérer avec la filière automobile dans le cadre de la relance. Le but de cette coopération était d'apporter des solutions technologiques, permettant d'accélérer l'introduction des véhicules à plus basse consommation d'énergie, en particulier les véhicules 100 % électriques, hybrides rechargeables ou micro-hybrides.

Nous développons des transistors de puissance spécifiques destinés à améliorer le rendement de la conversion de l'énergie du courant alternatif en courant continu destiné à charger les batteries. Une fois la batterie chargée, il s'agit de reconvertir, pour le moteur électrique triphasé, la tension continue de la batterie en courant alternatif. Nous travaillons sur des processus de conversion d'énergie en maximisant le rendement afin d'éviter les pertes en chaleur ou dans la conversion du système.

Grâce à ces avancées technologiques sur lesquelles nous travaillons actuellement, nous allons développer des solutions de chargeurs intégrés à bord des véhicules, sur les convertisseurs permettant de convertir cette énergie, voire sur les différentes tensions. Dans les véhicules électriques, la batterie principale se situe autour de 400 volts, et jusqu'à 800 volts sur les véhicules haut de gamme. La plupart des véhicules sont équipés d'une batterie 400 volts. La batterie 12 volts traditionnelle se convertit actuellement en une batterie 48 volts. Plus la tension monte, plus cela réduit l'intensité de l'ampérage et donc le diamètre des fils de

cuivre. La conséquence est une réduction du poids et de la chaleur. Avec les composants du type nitrure de gallium (GaN) que nous allons développer, cela réduira en outre le rendement thermique. Cela signifie qu'à l'avenir, nous n'aurons plus besoin de refroidissement liquide autour de l'électronique, comme les circuits de radiateurs classiques des moteurs thermiques existant actuellement. Dans le futur, le refroidissement s'opérera uniquement par air. Les conséquences sont des réductions du poids, de la consommation d'énergie et du prix. Cette solution avantageuse est en cours de développement.

Nous développons donc cet écosystème de façon transversale. Laissez-moi vous donner un exemple précis. Nous avons formulé des propositions dans le cadre du plan de relance et des 100 millions d'euros proposés à la filière automobile, en coopération avec des acteurs de cette filière. En France, ces acteurs sont Valeo, Vitesco, Renault ou encore PSA. Nous travaillons avec eux afin de créer des solutions permettant non seulement que les produits soient conçus et fabriqués en France mais également utilisés dans la fabrication des véhicules électriques.

Nous sommes environ à la moitié du plan Nano, démarré en 2018. Nous faisons des rapports annuels avec tous les acteurs. La feuille de route prévue dans le cadre du programme est respectée.

M. Philippe Latombe, rapporteur. Merci. J'aimerais vous poser deux questions avant de passer la parole à Mme Hoel. J'ai relevé un point sur la partie formation. Je ne vous interrogerai pas sur ce point maintenant. J'aimerais relever un point et vous poser une question à part.

Vous avez dit que le leadership de l'intelligence artificielle dans le *cloud* était plutôt détenu par les Américains. Vous avez également dit que nous disposons d'un avantage compétitif très fort et d'une véritable expertise sur l'intelligence artificielle décentralisée. Avons-nous définitivement « perdu le match » sur l'intelligence artificielle dans le *cloud* ou sommes-nous capables de rattraper notre retard ? En sens inverse, les Américains seraient-ils capables de nous rattraper plus facilement sur l'intelligence artificielle décentralisée en raison de leur expertise sur l'intelligence artificielle dans le *cloud* ?

Ma deuxième question concerne l'actualité d'ordre économique. ARM fait l'objet d'un rachat par Nvidia. Est-ce une mauvaise nouvelle ? Qu'en pensez-vous ? Que pouvez-vous nous en dire ?

M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique. Il est difficile de vous répondre sur le premier point car les acteurs français et européens ne sont pas positionnés. L'année dernière, le marché du semi-conducteur, des composants électroniques a représenté 440 milliards de dollars de marché mondial. Sur ce marché mondial, environ la moitié est destinée aux marchés des PC, des *smartphones* et des mémoires. Or les acteurs européens ne sont pas fournisseurs sur ces éléments. Les fournisseurs sont Intel, Qualcomm, Broadcom et les trois fabricants de mémoires dynamiques dans le monde. Nous ne sommes donc pas positionnés sur ces marchés.

La filière française et européenne se positionne principalement autour de l'automobile. Nous développons des composants dans différents domaines, que ce soit l'électronique de puissance – avec des technologies à base de carbure de silicium, de nitrure de gallium ou de transistors *Metal Oxide Semicondutor Field Effect Transistor* (MOSFET) – ou sur la partie digitale des automobiles. Il existe aujourd'hui une cinquantaine de microcontrôleurs dans un véhicule (des caméras, des radars, de proximité ou de longue distance). Le véhicule automobile est en voie de devenir beaucoup plus complexe qu'un PC. En termes de logiciels,

il s'agit dès à présent d'un facteur dix. La complexité de ce domaine nécessite des compétences spécifiques. STMicroelectronics et les acteurs européens sont très focalisés sur l'automobile, d'autant plus qu'il s'agit du marché ayant la plus forte croissance. Les marchés du PC et du *smartphone* connaissent aujourd'hui une croissance mondiale relativement faible. En revanche, le marché de l'automobile est celui qui connaît la plus forte croissance.

Par ailleurs, nous sommes fortement positionnés sur l'industrie 4.0 ou les objets connectés à travers des propositions de vente de solutions avec des microcontrôleurs 32 bits et des technologies de connectivité telles que le *Bluetooth Low Energy*, le WiFi, l'Ultra Wideband et le Narrowband IoT (NB-IoT). Le NB-IoT représente l'évolution des technologies 5G pour les objets connectés. Chez STMicroelectronics, nous utilisons des cœurs ARM pour la fabrication de ces microcontrôleurs 32 bits. Toutes ces technologies de connectivité, les microcontrôleurs ainsi que les capteurs (soit des caméras soit des capteurs de proximité ou de positionnement) nous permettent de maintenir une bonne position sur l'offre auprès des acteurs européens dans le domaine de l'industrie 4.0 ou des objets connectés.

Nous sommes également bien positionnés dans le domaine des imageurs, c'est-à-dire la reconnaissance à travers des caméras sur des solutions de reconnaissance faciale par exemple.

Le positionnement de STMicroelectronics et des différents acteurs au niveau européen est celui-ci.

Sur le sujet de l'intelligence artificielle embarquée, il faut distinguer plusieurs axes. Aujourd'hui, des solutions existent dans le domaine des véhicules autonomes. Le marketing autour de ces véhicules est abondant. Les solutions retenues sont dites « de voitures autonomes », permettant de garder le véhicule sur la voie empruntée. Ces solutions évolueront vers davantage d'autonomie et de complexité, avec des composants permettant la fusion des données. En effet, ces composants puiseront dans les informations issues des caméras ou encore des radars de longue distance. Par exemple, il s'agit de savoir si le véhicule situé devant freine. Il existera aussi une connexion des informations, soit à travers les réseaux 5G soit à travers des réseaux WiFi de communication de véhicule à véhicule. Il existe donc beaucoup de données et une fusion des informations.

Deux acteurs jouent un rôle dans la fabrication des composants : l'entreprise américaine Nvidia, qui possède des puissances de calcul importantes mais aussi une très forte consommation d'énergie, et STMicroelectronics, qui fournit environ 70 % du marché mondial dans ce domaine. Ce fait est souvent méconnu mais les composants de STMicroelectronics sont développés et fabriqués en France, dans l'usine de Crolles, avec une technologie basse consommation 70 nanomètres. Un client israélien de STMicroelectronics revend ces produits aux fabricants de voitures ou aux équipementiers de premier rang. Ce client détient 70 % du marché mondial.

Ce positionnement est donc intéressant dans le domaine du véhicule automobile. Nous travaillons sur des évolutions, avec des composants beaucoup plus puissants, capables de dizaines de téra d'opérations par seconde pour le véhicule automobile.

Concernant le *Edge Computing*, soit l'intelligence artificielle décentralisée, nous travaillons avec les différents acteurs pour développer des microcontrôleurs et des microprocesseurs 32 bits intégrant à la fois les cœurs ARM et les accélérateurs. En effet, dans le cadre de l'intelligence artificielle embarquée, il est nécessaire de télécharger les algorithmes spécifiques (l'ensemble de ce que vous pouvez faire avec des réseaux de neurones) et de faire les calculs avec une grande rapidité tout en consommant peu d'énergie électrique. C'est ce que

nous développons aujourd'hui dans les *roadmaps* que nous avons produites, en coopération avec les personnes développant les logiciels. Cela fait partie des groupes de travail avec le CEA-Leti dans le cadre du plan de filière sur l'intelligence artificielle embarquée mais aussi des développements de produits que nous menons en France dans ce domaine.

Afin de vous donner un ordre de grandeur, je note que STMicroelectronics est le numéro deux mondial des microcontrôleurs 32 bits. Depuis le début de cette opération, nous avons livré plus de 6 milliards de pièces, principalement fabriquées en France. Notre positionnement est très fort. Nos clients sont plus de 60 000 dans le monde. Nous voulons utiliser cette base installée pour offrir des microcontrôleurs mais aussi des capacités d'intelligence artificielle décentralisée. Nous restons donc sur la décentralisation, dont nous pensons qu'elle constitue une opportunité en France et en Europe car nous avons, tout de même, quelque peu perdu l'intelligence artificielle dans le *cloud*. Il sera très difficile de revenir sur des marchés purement digitaux, purement « serveurs » à moyen terme car nous n'avons pas le *know-how*, le savoir-faire, et parce que nous ne pouvons pas nous diversifier. Il s'agit d'un sujet difficile pour nous car nous ne pouvons pas revenir en arrière sur le digital. En effet, cela fait trente ans que les fournisseurs sont américains. Nous ne sommes pas sur le marché du PC. En revanche, nous sommes sur les marchés des équipements finaux, des objets connectés, de l'industrie 4.0, *etc*. C'est dans ces domaines que nous détenons une véritable opportunité.

En France, nous sommes dotés de grandes compétences dans le domaine de l'algorithmique. Un grand nombre des diplômés des écoles d'ingénieurs ou des universités partent travailler vers des sociétés américaines, dont je ne citerai pas les noms. Nous avons donc cette possibilité. L'enjeu sera de réussir à faire travailler les écosystèmes car le *soft* et le *hard* constituent deux métiers différents – presque deux « mondes » différents, si je puis dire. L'objectif de la filière et des actions que nous menons est de créer cette synergie, avec les services de la DGE en particulier, entre les laboratoires qui développent cette technologie, les fabricants de *hardware* et les équipementiers terminaux.

Je vous donne un exemple. Aujourd'hui, dans l'agriculture, des personnes souhaitent développer l'agriculture sélective. Une caméra serait installée sur un tracteur, avec de l'intelligence artificielle embarquée, afin de savoir s'il est nécessaire de traiter ou non un pied de vigne. Soit l'agriculteur descend de son tracteur et regarde si le pied de vigne nécessite un traitement, soit cette analyse est réalisée automatiquement, *via* une caméra, par des logiciels d'intelligence artificielle déterminant s'il faut déverser ou non de l'engrais ou des produits phytosanitaires. Cela constitue un bon exemple de ce qu'est l'intelligence artificielle embarquée. Dans ce domaine, le champ d'application est infini. Cette intelligence artificielle doit bien sûr être raisonnable et suivre les directions données par les rapports de la commission européenne dans ce domaine.

Nos opportunités se trouvent donc dans ce domaine. Dans le domaine pur du *cloud*, il me semble très compliqué de revenir en arrière.

Le deuxième sujet concerne la société anglaise ARM, ayant développé des cœurs de microcontrôleurs. Aujourd'hui, il s'agit du leader mondial des cœurs. Les STM 32, comptant 6 milliards de composants dont je vous ai parlé précédemment, utilisent des cœurs ARM. Nos concurrents européens utilisent également des cœurs ARM. Nous utilisons tous des cœurs ARM, à la fois dans les objets connectés et dans les futurs produits pour l'automobile. Il s'agit donc d'un sujet extrêmement stratégique. Cela fait partie de l'évolution des chaînes de valeur existant dans le domaine de l'électronique.

Comme vous le savez, ARM a été racheté par la société japonaise SoftBank il y a trois ans. Cette société a annoncé vouloir vendre ARM au concurrent américain Nvidia. Tout le monde se pose des questions, notamment sur les autorisations qui seront données ou non pour cette acquisition. En effet, des processus sont nécessaires auprès de la direction générale de la concurrence en Europe et dans d'autres pays, afin de donner l'autorisation pour cette acquisition. Deuxièmement, des questions existent sur les conséquences de cette fusion.

Aujourd'hui, les informations que nous avons auprès des sociétés comme ARM, Nvidia ou SoftBank nous rassurent sur la pérennité des solutions et des feuilles de route qu'ils suivent actuellement. Néanmoins, je ne peux pas vous renseigner davantage sur le degré d'engagement qui sera tenu à ce propos. Il est certain qu'en cas de divergence à moyen terme des développements de cette société par rapport aux besoins de l'industrie française ou européenne, cela poserait grandement problème car il n'existe pas beaucoup, voire pas du tout, d'alternatives à ce jour.

La fusion d'ARM est donc un vrai sujet concernant la souveraineté numérique. Un corollaire découle de ce sujet. Vous savez qu'il existe des tensions géopolitiques fortes dans le domaine des composants. Vous avez dû voir que l'administration américaine a mis en place une licence d'exportation vers un client chinois. STMicroelectronics fournit ce client chinois, l'un des dix premiers clients de la société. Cette information est du domaine public. La troisième réglementation nous impose de demander une licence dans la mesure où nous utilisons un équipement d'origine américaine (soit dans le développement soit dans la production). Dans le domaine des composants électroniques, cette demande de licence est obligatoire. En effet, les étapes de production sont tellement complexes qu'il n'existe pas de monopole ou de seconde source possibles dans ce domaine. Nous avons donc des fournisseurs monopolistiques américains, européens, japonais, *etc*. Nous sommes obligés de travailler avec tout le monde dans ce domaine.

Nous sommes donc contraints de demander une licence d'exportation et nous allons suivre les réglementations. Les conditions d'acceptation ou de refus de cette licence ne sont pas claires. La durée de l'obtention d'une réponse n'est pas claire non plus. À ce jour, et depuis le 17 septembre, les livraisons ne sont plus possibles vers ce client chinois. C'est impossible même si nous voulons livrer depuis l'usine de fabrication de Crolles jusqu'au client chinois à Paris. Il existe donc une extraterritorialité forte dans ce domaine, stratégique. Je ne ferai pas de commentaires sur les raisons derrière tout cela. Néanmoins, il est clair que, s'il s'avérait que ARM était acquise par une société américaine, la problématique de la licence d'exportation pourrait être élargie à d'autres clients aussi. Il s'agit d'un sujet sur lequel nous sommes très favorables à une application stricte des règles de l'Organisation mondiale du commerce (OMC).

Vous avez vu que les 444 milliards de dollars de chiffre d'affaires des composants électroniques constituent un enjeu majeur. J'imagine que votre rapport le reprendra. Aujourd'hui, les grandes puissances mondiales veulent maîtriser la chaîne de valeur des composants électroniques. Historiquement, les Américains ont eu un leadership très fort, qu'ils ont ensuite quelque peu perdu au profit des Coréens, des Taïwanais et des Européens. Je considère que le positionnement des acteurs européens STMicroelectronics, Infineon et NXP, en particulier dans le domaine automobile, relève d'un leadership mondial. Sur les segments de marchés sur lesquels nous nous situons, nous sommes donc assez forts. L'année dernière, STMicroelectronics a été le huitième fournisseur mondial de composants électroniques, suivant certains rapports. Nous avons donc des positionnements forts. Il existe aussi des endroits où nous ne sommes pas présents. Il n'est pas possible de revenir dans ces lieux car les barrières sont colossales à l'entrée. Il faut donc être forts dans les secteurs où nous sommes

déjà bien implantés. Nous devons également avoir une stratégie de diversification. L'intelligence artificielle embarquée en est une en particulier.

La stratégie d'acquisition d'ARM constitue un vrai sujet, sur lequel nous n'avons pas les réponses. Le sujet corollaire concerne ces enjeux géopolitiques et les financements menés par les différents États. Nous avons parlé du PIIEC et du plan Nano en France, représentant un milliard d'euros pour tous les acteurs pendant cinq ans. À travers son plan China 2025, la Chine a décidé de dépenser 150 milliards de dollars sur les composants électroniques. Les États-Unis discutent du lancement d'un plan de rattrapage de l'ordre de 20 ou 30 milliards de dollars – les chiffres ne sont pas encore précisément connus mais ils sont assez importants. Bien sûr, concernant le *Defense Advanced Research Projects Agency* (DARPA), nous ne détenons pas beaucoup d'informations sur les financements associés.

Ces sujets constituent donc de vrais enjeux. En 1973, le pétrole représentait un enjeu mondial. Nous pouvons dire que les composants électroniques constituent une partie des enjeux géopolitiques et stratégiques majeurs.

Mme Virginie Hoel, professeure des universités. Je souscris totalement à tout ce qui a été dit. Je pense que l'État français doit se rendre compte que la perte des composants peut « tuer une économie ». Il me semble que c'est un sujet primordial. Le rôle de la filière est aussi de prévoir et d'anticiper tous les nouveaux marchés et de permettre un développement de l'économie.

Au niveau de la filière, nous développons tout un axe autour des compétences, afin de répondre à l'ensemble des enjeux stratégiques qui se trouent devant nous. De très grandes attentes existent de la part des industriels. J'aurais une position assez optimiste, en disant que ces industriels sont encore présents sur le territoire. Ces compétences peuvent toujours être « réanimées » mais sont en voie de disparaître. De nombreux départs à la retraite ne sont pas remplacés. Des compétences considérables sont en train de disparaître.

Par ailleurs, le champ de l'attractivité est important. À mon sens, l'électronique a souffert d'un manque d'attractivité par rapport au numérique. Les solutions matérielles ont été quelque peu victimes du succès du numérique. L'électronique n'était plus très « à la mode ». Pourtant, sans solution matérielle, il n'est pas possible de développer des solutions numériques dignes de ce nom.

Le manque d'attractivité concerne notamment les jeunes filles. Je suis un contre-exemple, même si je ne suis plus très jeune. En termes de féminisation de la filière, seuls 20 % de filles sont attirées par les sciences en général. Nous sommes impliqués sur ce sujet.

Comme l'a dit Thierry Tingaud, nous essayons de créer des discussions entre les écosystèmes. C'est ce que nous tentons de faire au sein de la filière, en mobilisant à la fois les acteurs de l'enseignement supérieur, de l'éducation nationale et les industriels afin que chacun puisse identifier les différents sujets et mettre en place des actions. Dans ce cadre, nous avons formé un groupe de travail impliquant tous les champs. Ce groupe de travail est composé de directeurs des ressources humaines (DRH), d'acteurs de terrain au niveau industriel, d'enseignants-chercheurs, d'acteurs de la formation continue comme l'Agence nationale pour la formation professionnelle des adultes (AFPA) et des représentants du ministère de l'emploi. Nous regroupons donc toutes ces différentes composantes. Nous avons identifié plusieurs actions à mener.

Cette démarche a aussi lieu dans le cadre d'un Engagement développement et compétences (EDEC). Nous avons été lauréats au niveau de la filière pour ce projet. Ce projet

se mène aussi avec la photonique, secteur qui rencontre les mêmes problèmes que nous. Dans le cadre de cet EDEC, nous disposons d'environ 500 000 euros à partager avec la photonique sur quatre grands axes.

Dans le but que nous soyons certains de bien dimensionner le projet et l'offre de formations, le premier axe vise à réaliser une cartographie dynamique des métiers en tension. De grands besoins existent actuellement. Il n'est plus possible de trouver certains opérateurs et certaines compétences considérables sur le marché. Il existe donc des besoins criants, notamment dans les domaines de l'analogique, de la technologie et du *hardware*. Ces besoins sont identifiés. Nous recevrons les résultats de cette cartographie en novembre. Globalement, tous les signaux repérés à la construction de la filière sont vérifiés et seront confirmés par l'étude menée dans le cadre de cet EDEC.

Le deuxième grand sujet est l'alternance. Nous travaillons pour développer cette alternance. Nous avons un autre sujet sur les formations initiales et formations continues. Nous souhaitons diversifier les offres de formation et amener, le plus rapidement possible, les compétences et les personnes sur les postes actuellement ouverts au niveau industriel.

M. Philippe Latombe, rapporteur. Merci. Je me permettrais de vous poser deux questions sur la partie formation. Objectivement, quels sont les meilleurs pays en termes d'enseignement de l'électronique ? La France et l'Europe sont-elles bien classées ? Nous voyons passer des classements, qui valent ce qu'ils valent.

Mme Virginie Hoel. Le classement de Shanghai ?

M. Philippe Latombe, rapporteur. Oui. Je veux dire que les classements ont la valeur qu'on leur donne. Néanmoins, ils reflètent une certaine réalité. Disposons-nous du meilleur enseignement ou de l'un des meilleurs enseignements au monde dans ce domaine ?

J'aimerais vous poser une deuxième question. Selon vous, est-ce que la création d'une sorte d'école européenne ou de filière européenne de l'enseignement dans ce domaine aurait du sens ? Une telle création pourrait-elle susciter une « force de frappe » et de l'attractivité ? Permettrait-elle de profiter de l'attractivité d'autres pays européens, supérieure à la nôtre dans ce domaine ?

Mme Virginie Hoel, professeure des universités. Concernant le classement de Shanghai, ma réponse est affirmative. En France, il existe de très bonnes écoles et universités représentées dans ce classement. Il me semble que c'est Orsay qui fait partie des dix meilleurs établissements actuellement au niveau ingénierie et électronique. Je pense que nous avons de très bonnes compétences qui, de plus, sont particulièrement recherchées par les pays extérieurs. Nous formons très bien les étudiants. Je pense qu'ils sont très contents de la formation reçue. Bien souvent, ces étudiants vont se vendre ailleurs et font progresser des secteurs d'activités entiers chez nos concurrents. Il faut en prendre conscience.

Des laboratoires de recherche sont vraiment des pépites. À mon avis, ils sont sous-exploités au niveau du territoire. D'excellents docteurs sont formés dans ces laboratoires, ainsi que des spécialistes, pas assez reconnus non plus au niveau national.

Concernant la création d'une école européenne, il s'agit en effet d'une option. Je pense que nous pouvons retrouver le même niveau de compétences dans différents pays. Par exemple, l'Allemagne a la même approche et la même structuration que nous au niveau de la recherche même si leurs mécanismes sont quelque peu différents. J'avais personnellement participé à des projets européens, menés par le secteur de la défense, avec sept ou huit

partenaires européens ayant exactement les mêmes ambitions et la même façon d'aborder l'électronique que nous.

M. hierry Tingaud, président du Comité stratégique de la filière Industrie électronique. Si je puis compléter ce que vient de dire Virginie Hoel, j'ai l'expérience d'avoir fait travailler des équipes de développement en France, en Inde ou en Chine. Le niveau intrinsèque des ingénieurs européens est très bon. Nous manquons de bras mais le niveau de compétences et de capacité à résoudre un problème compliqué est fort. Cela est moins le cas en Inde et en Chine où les ingénieurs sont plus nombreux mais disposent de moins de capacité de résoudre des problèmes compliqués. En Inde et en Chine, les ingénieurs disposent plus de la capacité de reproduire ce qu'ils ont appris que de celle de découvrir des choses. Cela tient vraisemblablement au mode d'apprentissage dans l'éducation française. Nous disposons donc vraiment de compétences.

J'ajouterais l'importance cruciale du crédit d'impôt recherche (CIR) si l'on veut maintenir de la recherche et du développement en France. C'est absolument fondamental. Dans une entreprise comme STMicroelectronics, dont l'effectif s'élève à 46 000 personnes dans le monde, un tiers des effectifs travaille dans la recherche et le développement. Naturellement, à chaque fois, vous regardez la balance économique par rapport au coût d'un ingénieur en Chine, en Inde, aux États-Unis ou ailleurs. L'impact du CIR est décisif.

M. Guillaume Adam, délégué du Comité stratégique de la filière Industrie électronique. Comme vous l'avez vu, notre filière est très mobilisée sur ces sujets de souveraineté numérique, avec un certain nombre de dispositifs de soutien français ou européens, évoqués pour certains ce matin. Nous avons notamment évoqué le PIIEC et le plan Nano 2022. Le PIA, qui arrivera dans sa version 4, est également très important pour notre secteur. Certains volets de ce plan concerneront directement les thématiques sur lesquelles nous travaillons, particulièrement l'intelligence artificielle ou le CIR. Il existe d'autres dispositifs que je souhaitais également mentionner, tels que le dispositif de la jeune entreprise innovante (JEI) et les programmes européens Horizon Europe et Digital Europe, dont nous sommes assez familiers. Ces deux programmes européens viennent utilement compléter les instruments pour accompagner l'industrie européenne, à la fois dans sa recherche et ses développements. Je me suis permis d'attirer votre attention sur ces différents dispositifs complémentaires, d'une importance capitale pour la filière.

M. Philippe Latombe, rapporteur. Merci. Au sujet de la souveraineté pour votre filière, quels sont les grands enjeux et menaces que vous pouvez voir ? Nous en avons évoqué plusieurs. Sommes-nous passés à côté de quelque chose ?

M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique. Je pense que nous avons évoqué les principaux enjeux et menaces. Nous voyons bien qu'il existe une prise de conscience des enjeux au niveau mondial, au sujet des composants électroniques. Cette prise de conscience est vraiment très forte. La Chine, les États-Unis mais aussi le Japon, la Corée et Taïwan consentent des investissements massifs pour avoir un leadership mondial dans ce domaine.

Je pense que nous possédons de réelles compétences en France et en Europe dans les domaines que j'ai mentionnés, pour le marché des nouveaux véhicules. Ce point est très important.

Nous sommes particulièrement focalisés sur l'offre de solutions pour contribuer à la transition écologique, en apportant beaucoup de régulations faites par des composants du type

microcontrôleurs afin de réguler et de réduire la consommation d'énergie. Cela fait aussi partie des axes stratégiques de l'entreprise.

Je pense que nous avons besoin de capitaliser sur nos points forts et d'avoir une stratégie d'élargissement de ces points forts. L'intelligence artificielle embarquée est typique. Nous devons continuer en ce sens.

Il faut veiller à ne pas se diversifier. Je sais qu'il existe aujourd'hui des réflexions sur la souveraineté purement numérique, c'est-à-dire « qu'en est-il des microprocesseurs ? » et « qu'en est-il des mémoires ? ». Par rapport à ce que vous disiez précédemment, monsieur le rapporteur, sur les enjeux de l'intelligence artificielle dans le *cloud*, ces éléments nous semblent très compliqués à réinitialiser sauf si nous pouvons travailler sur de nouvelles générations du type technologies quantiques. En effet, tout est ouvert sur ces nouvelles générations et il existe sans doute des compétences en France avec, entre autres, le Commissariat à l'énergie atomique et aux énergies alternatives (CEA). Il s'agit peut-être d'une voie à moyen terme ou à long terme, pour revenir sur ces aspects de processeurs numériques purs avec des technologies complètement différentes. Néanmoins, sur le digital traditionnel, cela me paraît compliqué.

M. Philippe Latombe, rapporteur. Imaginons que le « deal » ne soit pas une réussite entre ARM et Nvidia. Existe-t-il un acteur européen ayant la capacité de se porter acquéreur d'ARM ? Que manquerait-il aux entreprises majeures de la filière pour que celles-ci puissent se regrouper ? Vous l'avez dit vous-même, ARM fabrique le cœur de l'ensemble des composants que vous utilisez pour ensuite les revendre. Plutôt que de laisser passer son fournisseur principal et se mettre en position de dépendance, il pourrait être intéressant de se réunir à plusieurs afin de le racheter. Un tel rachat est-il faisable ? Que faudrait-il pour pouvoir l'effectuer ?

M. Thierry Tingaud, président du Comité stratégique de la filière Industrie électronique. Il est quelque peu compliqué pour moi d'évoquer ce sujet pour des questions de confidentialité. Des axes de réflexions de cette nature sont menés par la direction générale des réseaux de communication, du contenu et des technologies (DG CONNECT). Je ne peux pas en dire plus mais cela représente 40 milliards de dollars. Le sujet que vous évoquez n'est pas strictement européen. Je pense que la réflexion existe au Japon, en Corée, à Taïwan et à Singapour. Cette réflexion doit éventuellement être poussée davantage. Mais il est compliqué de s'inscrire dans un processus de rachat d'entreprise privée.

Mme Virginie Hoel. J'aimerais des précisions sur la suite de ces échanges.

M. Philippe Latombe, rapporteur. Nous sommes au début des auditions. L'idée est de voir clairement quelles sont les voies. C'est dans ce but que nous posions la question de l'intelligence artificielle dans le *cloud* et de l'intérêt d'y investir ou non. Vous avez parlé de diversification à ce sujet. Nous sommes au début des auditions, sachant que le rapport doit être rendu pour juin 2021. Nous sommes au début de la démarche et souhaitons baliser l'ensemble du champ. C'est pour cela que nous souhaitions vous auditionner très rapidement car, effectivement, de nombreuses informations ont été données sur le digital pur. Nous nous rendons compte que le digital sans le matériel ne fonctionne pas. Il était donc nécessaire de vous entendre au début, quitte à réorganiser éventuellement des auditions très spécifiques sur des points identifiés dans les semaines et mois à venir, afin de comprendre comment créer des synergies.

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 (8 octobre 2020)

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.

Audition, ouverte à la presse, de M. Henri Verdier, ambassadeur pour le numérique
(15 octobre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. Philippe Latombe, rapporteur. Nous sommes heureux d'accueillir aujourd'hui parmi nous notre ambassadeur pour le numérique, M. Henri Verdier. Monsieur Verdier, vous avez été nommé à ce poste en 2018 et votre mission consiste, je cite, à « *coordonner l'élaboration des positions de la France sur les questions internationales touchant la transformation numérique et à les promouvoir auprès de nos partenaires internationaux comme auprès des autres acteurs publics et privés* ». Notre mission d'information va, durant plusieurs mois, se pencher sur les moyens de bâtir et de promouvoir une souveraineté française et européenne. Nous souhaiterions connaître votre analyse de cette notion de souveraineté numérique, notamment la pertinence de l'échelon européen pour œuvrer à son développement. Nous sommes également intéressés par les conditions concrètes d'exercice de votre mission, les enceintes d'intervention, l'existence d'homologues dans les pays partenaires versus une spécificité typiquement française. La politique étrangère de la France en matière de numérique recouvre un grand nombre de questions essentielles telles que la cybersécurité, la neutralité d'internet, la protection des données personnelles, la lutte contre les *fake news* ou les discours de haine, le multilatéralisme ou encore la souveraineté européenne du numérique. Comment participez-vous à l'élaboration des politiques françaises sur ces différents sujets ? Et quelle est la coordination des différents services de l'État sur ces problématiques ?

Votre position contribue à la dimension croissante de l'action internationale de la France dans le domaine du numérique. Pouvez-vous nous rappeler sur quels principes généraux elle se fonde et les valeurs qui la guident ? Est-il de votre ressort d'assurer une cohérence au regard des multiples problématiques présentées et des divers canaux empruntés pour cette action ? Le numérique est en effet riche de sujets diversifiés présentant parfois des enjeux majeurs au regard de la place de la France sur la scène internationale, en particulier en matière de cybersécurité et de cyberdéfense. Dans ces domaines, la thématique de la souveraineté est prégnante puisqu'il s'agit de déterminer comment protéger les intérêts français de nouvelles menaces immatérielles et déterritorialisées. L'objectif est également de définir de nouvelles modalités de discussion avec nos partenaires, notamment européens, afin d'engager des actions concertées respectueuses de la souveraineté de chacun. Nous souhaiterions connaître la position de la France sur ce sujet, les enceintes de discussions autour de ces enjeux sécuritaires, ainsi que les partenaires privilégiés – l'Europe est-elle unie ? – et les principales négociations en cours dans les enceintes multilatérales.

La souveraineté numérique française et européenne est également confrontée, selon un mode sans doute moins conflictuel, à la montée en puissance d'acteurs privés qui prétendent imposer leurs normes et/ou disposent d'un pouvoir de marché les rendant souvent incontournables pour les consommateurs et les usagers. Comment, selon vous, la France et l'Europe peuvent-elles reprendre la main dans ces rapports nouveaux afin de ne pas être réduites à une situation seulement réactive, voire passive ? Nous pourrons ici évoquer les instances privées ou semi-privées où s'organise la gouvernance d'internet (pour l'attribution des noms de domaine par exemple). Nous pourrons discuter également des géants du numérique de plus en plus souvent prescripteurs, tant de nos modes de consommation que de nos modes d'information. La crise que nous connaissons ne fait que renforcer ces tendances. Quelle réponse publique apporter, selon vous, au plan national, européen et international ?

Enfin, la défense de la souveraineté numérique passe également par une certaine autonomie matérielle et par la défense et la promotion d'une industrie du numérique européenne, compétitive et indépendante. Or, l'Europe souffre de départs d'industries stratégiques pour le matériel informatique qui constitue pourtant le sous-bassement du développement du numérique. La dépendance aux solutions technologiques extracommunautaires, logicielles comme matérielles, met-elle selon vous en cause l'autonomie européenne ? Comment contrer ces tendances et comment faire participer l'innovation et la recherche à une forme de réindustrialisation dans les nouvelles technologies, afin d'assurer une plus grande souveraineté européenne ? Pourriez-vous revenir sur cet aspect de la diplomatie économique qui pourrait s'attacher à votre mission ?

Je vous laisse la parole et vous remercie d'avance pour vos réponses.

M. Henri Verdier, ambassadeur pour le numérique. Je vous remercie pour le vaste programme que vous proposez. Je vais répondre aux différentes questions posées. Hier, nos équipes ont échangé sur la base d'un conducteur que je vous invite à suivre. Dans un premier temps, j'évoquerai la diplomatie numérique et les attributions de l'ambassadeur pour les affaires numériques et aborderai la notion de souveraineté numérique que la France propose à l'Europe.

Avec le recul historique, il apparaît que les acteurs de la révolution industrielle d'il y a trois siècles ont exercé une domination durable sur l'ordre du monde, pour son bien (le progrès) ou son mal (la domination). Aujourd'hui, nous assistons à une nouvelle révolution industrielle et certains pays savent que leur destin, dans les trois prochains siècles, se joue dans la maîtrise de cette technologie. La transformation des modes d'échanger, commercer, apprendre justifie selon moi cette appellation de nouvelle révolution industrielle. Nous assistons à une course à l'hégémonie. Vous avez, monsieur Latombe, évoqué la plupart des dimensions de la souveraineté numérique, nous les compléterons en chemin. Ces dimensions sont très concrètes. Lors de l'attentat terroriste de Christchurch, en Nouvelle-Zélande, Facebook s'est interrogé pendant des heures sur la définition de terrorisme. À l'époque, les États-Unis ne reconnaissaient pas encore le *violent extremism* d'extrême droite comme du terrorisme et aucune définition internationale consensuelle du terrorisme n'existait.

Je rappelle que 90 % des applications de nos smartphones ont accepté les conditions de service d'Android et Apple, peut-être de Facebook Connect et Paypal, et certainement de Google Maps. Ces applications peuvent donc subir, du jour au lendemain, des modifications de leurs conditions de service. Par exemple, Google Maps a, en 2018, changé les tarifs de son interface de programmation d'application (*Application Programming Interface-API*) en les multipliant par 100 pour certains utilisateurs. Lorsque j'étais que DSI (directeur interministériel du numérique et du système d'information et de communication) de l'État, j'ai vu à l'époque des sous-préfectures fermer des sites, car elles n'étaient pas en mesure de les financer à hauteur de 3 000 euros par an. Cette situation crée de la vulnérabilité et une asymétrie, puisqu'à tout moment, les plateformes telles que Facebook Connect, Paypal ou Google Maps, en savent plus que la start-up à l'origine de l'application. La start-up n'a donc aucune chance de renverser le pouvoir de force. Je prends comme autre exemple les élections américaines. Leurs campagnes sont structurées par la publicité ciblée. Certains candidats vont dépenser jusqu'à un demi-milliard de dollars pour utiliser une base de données présentant 50 informations pour 200 millions d'Américains. Ainsi, 3 000 à 4 000 messages cibleront différents profils. D'après les sociologues, cette fragmentation de la vie publique n'est pas sans rapport avec la montée de la violence. En Europe, la publicité politique est encadrée, le financement des campagnes est limité et la vie privée protégée. Mais des forces privées sous-entendent que ce modèle est dépassé. Ces exemples illustrent le caractère très concret de

problématiques qui relèvent du choix du peuple souverain, tant pour les campagnes politiques qu'au sujet de la vie privée ou de l'*open data*.

Venons-en au rôle d'ambassadeur pour les affaires numériques. La révolution numérique détermine désormais lourdement la prospérité et la souveraineté des États, car elle est devenue un objet géopolitique important qui caractérise les relations entre États. Le droit du conflit et le droit humanitaire doivent quant à eux faire place à la question cyber. Par exemple, la guerre commerciale entre la Chine et les États-Unis détermine très lourdement l'avenir de l'économie mondiale et du numérique. En outre, les pratiques d'ingérence territoriale deviennent l'arme du pauvre et se répandent rapidement. Nous reviendrons sur l'Appel de Paris ou sur le partenariat mondial pour l'intelligence artificielle qui sont des coalitions d'initiative française instaurées afin de créer du dialogue entre États et faire émerger des réponses et des solutions. La révolution numérique pèse sur les relations internationales et pourrait amener les États à détruire la liberté d'entreprendre ou la liberté d'accès à la connaissance qui sont propres à la révolution numérique. La France doit peut-être rappeler que la révolution internet est celle d'innovateurs et d'entrepreneurs et qu'elle doit beaucoup à sa composition décentralisée, peu contrôlée, hostile au monopole. La ligne de force de la France repose sur la défense d'un internet libre, ouvert, sûr et unifié. Une fragmentation en internets régionaux à l'échelle du monde doit être évitée, car elle constituerait une mauvaise nouvelle pour l'économie, mais également pour la paix mondiale. En effet, l'accès à des informations par bloc continental engendrerait un affaiblissement de la compréhension mutuelle entre espaces géopolitiques et un accroissement des tensions.

Le numérique est, pour toutes raisons, devenu un objet diplomatique. Lors de ma prise de fonction au Quai d'Orsay, j'ai tenté de cartographier le territoire de la diplomatie numérique en dessinant une boussole représentant le périmètre de la diplomatie numérique. Le rapport d'activité correspondant est en ligne sur le site du Quai d'Orsay. Au sein du Quai d'Orsay travaillent cinquante responsables de différents dossiers numériques. Quatre sont responsables des négociations sur le droit international dans le cyberespace, deux sont en charge des retraits de contenus terroristes, une jeune femme a inventé le visa Start up, d'autres responsables traitent de l'aide au développement, de la politique culturelle, de la promotion de la francophonie, *etc*. La première mission de l'ambassadeur pour les affaires numériques est de donner une cohérence à une diplomatie numérique inventée pour faire face à un certain nombre d'enjeux. Notre boussole présente quatre axes.

Le premier concerne les enjeux de sécurité, de cybersécurité (sécurisation des infrastructures), de lutte contre les contenus étrangers hostiles, voire des contenus terroristes ou pédopornographiques qui appellent des décisions internationales. La France souhaite séparer la question de la protection des infrastructures de celle de la régulation des contenus. Certains pays ont au contraire pour stratégie une doctrine globale de guerre informationnelle qui rapproche ces deux dimensions. Dans le domaine de la cybersécurité, la France est très présente dans les instances onusiennes, dans des dialogues bilatéraux avec des alliés ou non alliés, dans la régulation des contenus avec des pays européens ou non européens. Le dialogue reste encore à inventer avec les grandes plateformes. La France s'implique fortement dans la gouvernance d'internet qui concerne pas moins de dix-sept instances qui ont vocation à standardiser et normaliser. L'ambassadeur pour les affaires numériques tient le siège de la France à l'ICANN (*Internet Corporation for Assigned Names and Numbers*) en charge du nommage internet, à l'*Internet Governance Forum* (que la France encourage à réformer pour émettre des préconisations), à l'OCDE (Organisation de coopération et de développement économiques), lorsque ce n'est pas Bercy, ainsi qu'au sein du G20, du G7 et d'un certain nombre d'institutions européennes.

Un deuxième axe de la boussole concerne les enjeux de diplomatie économique en lien avec le ministère de l'économie et des finances. Notre réseau diplomatique est au contact des French Tech. Le ministère de l'économie représente la France à l'OCDE dans les négociations sur la fiscalité du numérique. Il peut encourager des entreprises françaises dans leurs négociations avec de grands États. Enfin, dans le cadre de la diplomatie d'influence que j'appelle diplomatie de valeurs, la France défend depuis longtemps l'accès à la culture et à l'éducation, la liberté d'expression, la liberté de la presse, le développement des pays émergents, mais également, par exemple, la net-neutralité. Avec la révolution numérique, les politiques et les logiques d'action doivent évoluer, notamment pour défendre la francophonie ou réfléchir aux aides de l'Agence française de développement (AFD), et ce sans tomber dans la dépendance d'une grande puissance ni d'une grande entreprise. Nous accompagnons ces évolutions de politiques avec de beaux opérateurs tels que l'AFD ou l'Institut français.

Au centre de la boussole se trouve la fonction centre d'expertise. Nous sommes effectivement souvent la première équipe ayant la capacité technique pour effectuer des analyses sur la Libra (monnaie virtuelle), la blockchain (technologie de stockage et de transmission d'informations) ou l'IA (intelligence artificielle). Ces fonctions existent dans tous les pays homologues développés, mais elles sont rarement unifiées. En Allemagne, j'ai depuis quelques semaines une homologue directe qui est une ambassadrice numérique *at large*. Le *Tech Ambassador* danois était globalement sur le même périmètre, mais il envisageait de négocier avec les géants de la technologie quand la France les considérait non comme des États souverains, mais comme des forces économiques. Certes, de tels acteurs doivent faire partie de la solution, mais nous n'avons pas d'ambassade auprès des GAFA et ces derniers ont à New-York des bureaux commerciaux et non des ambassades. Hormis en Allemagne et en Suède, les compétences homologues sont fragmentées. Le réseau de la diplomatie cyber est pour sa part clairement identifiable. Il est composé d'ambassadeurs ou de hauts diplomates cyber et d'une représentation des pays dans la gouvernance d'internet. Cette dernière n'est pas toujours confiée aux affaires étrangères, elle peut relever du ministère de l'économie, de l'industrie, voire du ministère de l'intérieur pour les contenus à caractère terroriste.

Ce poste d'ambassadeur du numérique a une petite historicité. La diplomatie française était présente depuis une dizaine d'années dans la gouvernance d'internet et dans les sujets d'Open Gov (*Open Government Partnership*) et de cyber-négociation. Des responsables étaient en charge des différents dossiers. Puis, avec mon prédécesseur David Martinon, l'ambassadeur est devenu thématique, et nous continuons à muscler cette fonction. J'ai le privilège d'avoir une petite équipe de cinq collaborateurs, dont Louis-Victor de Franssu ici présent. Ils permettent de mettre en musique le travail des cinquante responsables du numérique au sein du Quai d'Orsay et d'avoir une approche matricielle. La lettre de mission que vous trouverez en ligne me donne la tâche de coordonner et représenter les positions françaises. Mais l'organisation du Quai d'Orsay est matricielle, avec éventuellement, pour chaque question numérique, un directeur géographique et un directeur thématique dont les apports sont importants. Notre travail consiste donc à sécréter une intelligence collective. Nous travaillons quotidiennement avec la direction de l'action stratégique et du désarmement, la direction des Nations unies, la direction générale de la mondialisation ou encore la direction de l'Union européenne. Le travail est conséquent à l'intérieur du quai d'Orsay, mais il est également interministériel pour chaque axe de la boussole.

Je travaille également au quotidien, selon les dossiers, avec le ministère de l'économie et des finances, le SGDSN (Secrétariat général de la défense et de la sécurité nationale), le SIG (Service d'information du Gouvernement), le ministère de l'intérieur, le ministère de la justice, le ministère des armées et le ministère de la culture. Je suis disponible pour répondre

à vos éventuelles questions à ce sujet. En tant qu'ancien directeur interministériel, j'ai découvert que la coopération des ministères régaliens était parfois plus fluide que les rencontres avec la DINSIC (direction interministérielle du numérique et du système d'information et de communication) dans le cadre de tâches plus civiles. Aujourd'hui, sous la houlette bienveillante du SGDSN, l'action interministérielle semble efficace sur les sujets de sécurité, de cyber, de retrait de contenu terroriste et de lutte contre les ingérences étrangères.

Abordons maintenant la question des enceintes privilégiées d'exercice de ces fonctions. La liste est longue et je transmettrai à la commission une liste exhaustive. De nombreux dossiers sont traités au sein de l'Union européenne comme les retraits de contenu terroriste ou le *Digital Services Act* (DSA) qui sera prochainement scindé en deux actes. Un plan de protection des démocraties est en préparation, un dialogue avec les grandes entreprises passe par le *European Internet Forum*, un groupe travaille sur les menaces hybrides, le service de l'action extérieure de l'Union européenne (SAE) avait souvent le leadership sur les questions d'ingérence, mais nous avons quelque peu modifié cette position. Ainsi, de nombreux enjeux sont traités au niveau européen. D'autres se jouent au sein de l'Organisation des Nations unies (ONU). Par exemple, le dialogue sur la cybersécurité et le consensus sur le droit international sur le cyberespace sont traités par deux groupes de travail. L'un est d'initiative américaine (groupe composé d'experts gouvernementaux) et l'autre est d'initiative russe (groupe à composition illimitée). Ayant observé que les deux groupes avaient fini par se paralyser, nous en proposons un troisième qui sera instauré une fois les travaux des deux groupes actuels finalisés. Le futur groupe de travail unique sera nommé *Program of action* et visera à changer les termes mêmes du débat sur le cyber.

La question de la gouvernance d'internet est très onusienne et nous avons participé aux différents IGF (*Internet Governance Forum*) et aux travaux lancés par le Secrétaire général des Nations unies. Nous pesons pour que l'*Internet Governance Forum*, enceinte multi-parties prenantes, soit renforcé, tranche sur ses propres débats et reconnaisse une place aux États. Si la culture de la *Permissionless Innovation* a bénéficié à internet, nous avons des responsabilités et des prérogatives en tant qu'État. Sans État souverain, la liberté individuelle est moindre, d'autant plus dans un monde de monopoles géants, de surveillance de masse et d'innovation débridée. Nous avons donc des choses à dire. Cette année, l'ICANN a failli prendre une décision qui nous a semblé grave, ce dont vous pouvez prendre connaissance en faisant des recherches sur la Toile. Malgré l'avis négatif quasiment unanime de ses membres, l'ICANN a voulu privatiser le .org et le vendre à un fonds d'investissement prêt à payer 1,5 milliard de dollars, sans pouvoir justifier de l'origine de ces fonds. Ce fonds pensait recruter l'ancien directeur de l'ICANN à l'origine de ce mouvement de privatisation. Le gouvernement français est la seule instance qui a souhaité stopper la démarche. À défaut de pouvoir recourir aux statuts, la France a usé de diplomatie en plaidant, justifiant, posant des questions et en se trouvant des alliés. Le procureur de Californie a joué un rôle clé en signalant que l'organisation qui depuis vingt ans était *non-profit* et donc ne payait pas d'impôts deviendrait sans doute, de par la vente envisagée, *for profit* impliquant le paiement d'arriérés sur vingt ans. Ce point a aussi contribué à empêcher cette vente. Certes, certains acteurs civils ne souhaitent pas que les États interviennent. Mais cet exemple montre que les procédures, la transparence et l'éthique ont été défendues par un gouvernement qui a agi non pas en tant qu'État auquel obéir, mais en tant qu'acteur du débat défendant des positions.

Nous travaillons beaucoup sur le sujet de la cybersécurité au sein de l'OCSE (Organisation pour la sécurité et la coopération en Europe). En outre, de nombreux travaux sont menés avec l'OCDE, en particulier un travail très intéressant sur la responsabilité du secteur privé dans la cybersécurité. Nous en sommes un peu à l'origine avec l'Appel de Paris sur lequel je reviendrai dans un instant. Nous pensons qu'une sécurité durable ne sera pas

créée uniquement avec du droit international. Un internet stable et sûr nécessite une montée en qualité des infrastructures et des services numériques qui sont de la responsabilité des entreprises qui les vendent. Nous travaillons également avec l'OCDE sur les rapports de transparence volontaire que nous nommons rapports d'auto-évaluation. Nous considérons que la réception d'un rapport annuel des entreprises concernant les réseaux sociaux ne suffit plus. Un échange de données est à construire afin de vérifier les éléments selon une approche consensuelle. Nous traitons d'autres dimensions de notre boussole au sein de l'Organisation internationale de la francophonie. Nous sommes présents à l'UIT (Union internationale des télécommunications) où se jouent des enjeux déterminants pour internet. Sur proposition de la société Huawei, un groupe de travail y a été créé pour un nouveau protocole TCP/IP que Huawei trouve plus rassurant, car il est plus clair, centralisé et mieux contrôlé.

Par ailleurs, nous menons des dialogues stratégiques serrés avec différents partenaires internationaux, les États-Unis, le Royaume-Uni, l'Inde, Israël, le Japon ou encore la Russie. Nous participons aux enceintes de discussions des entreprises d'internet telles que l'ICANN, l'IGF ou le GIFCT (*Global Internet Forum to Counter Terrorism*). Le GIFCT est la structure dont se sont dotées les entreprises de la Silicon Valley pour synchroniser les retraits de contenus terroristes une fois flagués. Je rappelle qu'après l'attentat de Christchurch, les tentatives de repostage ont la semaine suivante atteint le million sur Facebook et 400 000 sur YouTube. Une base de données et des outils sont nécessaires pour filtrer très rapidement les messages. Le filtrage se fait après flaguage par la police et retrait une première fois du post, afin d'empêcher sa republication. Suite à l'attentat de Christchurch, la France a plaidé pour et obtenu une réforme profonde de ce GIFCT qui a été doté d'une structure indépendante, d'un directeur dédié et d'un *advisory board* ouvert à cinq États et cinq représentants de la société civile.

Pour illustrer d'autres initiatives françaises, nous avons porté et négocié l'Appel de Christchurch, mon bureau est très présent sur ce sujet. Ainsi, des États, des entreprises et des représentants de la société civile s'organisent pour assurer le retrait des contenus terroristes en ligne. Je suis fier du travail accompli avec la Nouvelle-Zélande, car nous avons construit des règles d'États de droit. Cet Appel a engendré des résultats, notamment la réforme du GIFCT. Chacun a son rôle. Les États ne cherchent pas à supprimer des réseaux les contenus qui ne leur conviennent pas, mais à s'organiser pour détecter et signaler ces contenus. Les entreprises ont le devoir de les retirer en moins d'une heure et d'assurer la transparence. Enfin, la société civile veille à ce que les États légifèrent correctement et respectent les droits de la défense. Ces acteurs peuvent également aider à détecter les contenus terroristes. Aujourd'hui, le bilan est tout à fait positif, un équilibre a été trouvé.

L'Appel de Paris pour la confiance et la sécurité dans le cyberespace a été lancé en 2018. Cette organisation est devenue la plus importante en matière de cybersécurité, 78 États l'ont soutenue ainsi que des *local authorities* (incluant de grandes villes, l'État de Washington et l'État de Californie), 650 entreprises et 350 organisations non gouvernementales (ONG). Cet Appel permet d'illustrer l'unanimité internationale en matière d'application du droit international pour le cyberespace. Nos positions n'étant pas toujours majoritaires à l'ONU, il est précieux de pouvoir afficher le soutien d'entreprises et de la société civile. Ce fonctionnement a permis d'ouvrir un dialogue sérieux sur la responsabilité des acteurs systémiques, puisque la sécurité commence dans le design des solutions et les pratiques quotidiennes.

Bien sûr, la cybersécurité vise à empêcher des puissances étrangères de nous nuire. Mais, elle consiste également à expliquer aux fabricants d'objets communiquant que livrer des objets ayant pour mot de passe par défaut « adminadmin » est tout simplement criminel. Les

hackers savent que tous les utilisateurs ne vont pas changer leur mot de passe et ils en profitent. La divulgation responsable des failles est un autre sujet. Communiquer en conférence internationale sur une faille identifiée au sein d'une entreprise n'est pas un comportement intelligent. L'entreprise concernée doit avoir le temps de corriger la faille et d'implanter un patch.

La question de la souveraineté numérique, notamment européenne, est au cœur de ces problématiques, car notre souveraineté peut être menacée par des puissances étrangères, prise en otage dans des conflits continentaux ou encore menacée par des monopoles économiques. Laure de La Raudière le sait, j'ai créé ma première entreprise internet en 1995. À cette époque la France ne comptait que 15 000 internautes et Google et Facebook n'existaient pas. La révolution internet est porteuse d'émancipation, d'accès à la culture, de capacités de créer et d'innover. Les fondateurs d'internet évoquaient un *people empowerment*, soit un partage de puissance d'action. La souveraineté, pour favoriser ces capacités de créer, doit imposer des règles pour protéger les droits individuels qui sont connectés aux droits collectifs. Le ministre de l'Europe et des affaires étrangères, Jean-Yves Le Drian, s'est emparé de cet enjeu majeur qu'il porte. Vous trouverez en ligne son discours de Prague (décembre 2019) et son intervention à la conférence des ambassadeurs néerlandais (janvier 2020).

Nous pensons que la souveraineté française ne s'entend qu'en harmonie avec une souveraineté européenne. Un des grands combats est de convaincre nos partenaires européens que ce sujet est prioritaire et appelle une réponse politique. Parler de souveraineté numérique et de souveraineté numérique européenne n'était pas une évidence il y a trois ans. Les positions ont évolué. Peut-être la France a-t-elle trop souvent brandi l'étendard de la souveraineté pour défendre des entreprises, proches du pouvoir, en difficulté, ou une pulsion protectionniste. Nous en pâtissons aujourd'hui et devons en tirer les leçons. Toutefois, le fond de l'analyse demeure. Pour être souverain, un pays peut choisir le protectionnisme, derrière un *firewall,* ou l'hégémonie. La France propose une troisième voie qui est celle de l'autonomie stratégique pour prendre nos propres décisions sur la régulation de la vie privée, avoir une politique industrielle, décider d'une doctrine nationale de cybersécurité et interdire certains prestataires. Cette conception n'étant ni protectionniste ni hégémonique, elle ne rivalise avec aucun pays. La France peut ainsi être souveraine avec l'Allemagne ou l'Espagne. Elle peut également montrer aux partenaires en Afrique ou en Amérique latine que ce modèle permet des coalitions et des coopérations. Il est important d'entendre que ce récit de souveraineté est un récit d'autonomie stratégique. Durant ce cycle d'audition, des intervenants confondront peut-être la souveraineté avec l'intégration verticale d'une filière industrielle française. Or, un capital français n'est pas une garantie d'autonomie, car le cadre juridique ou technologique peut engendrer une privation de liberté de manœuvre. La possibilité de changer de prestataires peut tout à fait faire partie d'une stratégie de souveraineté.

Comme l'a dit Jean-Yves, Le Drian, la diplomatie française considère que pour atteindre l'ambition de souveraineté, quatre dimensions sont importantes. La première dimension est la sécurité et la cybersécurité. Vos travaux montreront que le sujet de la souveraineté est souvent né en marge de politique de régulation de la concurrence ou de politique industrielle, et a régulièrement tourné autour des questions de libre-échange et de protectionnisme. De fait, les problématiques liées à la sécurité, traitées au sein d'autres enceintes, sont souvent négligées. Pourtant, un pays qui risque d'être « débranché » en un claquement de doigts ne peut être considéré comme souverain. Un pays qui donne le code source de ses installations électriques à une puissance étrangère n'est pas non plus souverain. L'autonomie en matière de cybersécurité est pour nous la condition première de la souveraineté. Dans ce domaine, de multiples progrès restent à faire par l'Europe pour se protéger. Circonscrire les discours de haine tout en respectant la liberté d'expression est délicat

et impose d'interroger le *business model* de l'économie de l'attention et de la publicité personnalisée. Les *business models* des géants de la Tech doivent être confrontés, mais un État ne peut s'y attaquer seul. La cohérence et la réflexion sont pour cela de mise.

La deuxième dimension est la puissance de création. Dans le domaine du numérique plus qu'ailleurs, les inventeurs donnent le la. Personne n'aurait pensé à réguler le *search* ou les réseaux sociaux avant que ceux-ci n'existent. Les créateurs et les innovateurs sont toujours des forces, mais dans le secteur numérique, ils inventent les territoires mêmes de la régulation. Donc un pays qui ne crée rien est difficilement souverain. Une politique au service de l'innovation, au service de l'entrepreneuriat, au service de la croissance des entreprises est essentielle et indispensable. Je pense que nous partageons le constat d'une nécessaire économie du numérique. J'ajouterais que la puissance de création n'est pas l'apanage des entreprises. Les pays rayonnent et prennent aussi un *leadership via* leurs créations culturelles, l'impact de leurs intellectuels, le poids de leur recherche. En regardant une carte du monde, nous verrions que les pays disposant d'un écosystème numérique digne de ce nom ont notamment développé un cinéma national. En effet, ces pays pensent leur destin selon leurs valeurs et leur culture et ils ont le courage de choisir des chemins. Ainsi, la stratégie de puissance de création peut aussi passer par la culture et la recherche. La puissance californienne réside beaucoup à San Francisco, mais elle est également à Los Angeles. Et l'économie numérique de San Francisco a su profiter de l'industrie de contenus présente 800 kilomètres plus bas.

L'Europe s'est découvert la capacité d'être une puissance normative. Le règlement général sur la protection des données (RGPD) est, par exemple, devenu un vrai standard international. La Californie a adopté une loi de protection des données très similaire, le Mexique également, tandis que le Japon a obtenu un accord d'adéquation et que l'Inde finalise une loi de protection de la vie privée qui ressemble beaucoup au RGPD. Aujourd'hui, le plus grand marché mondial est constitué de consommateurs sous protection de type RGPD. Les entreprises européennes y gagneront un avantage compétitif puisqu'elles seront nativement prêtes pour le régime juridique le plus consensuel. Le Quai d'Orsay est convaincu que nous sommes capables de dupliquer cette force pour d'autres dossiers. Certains acteurs pensent que les États-Unis géreront les entreprises et l'Europe, la régulation. Une telle dissociation est impossible. Des intellectuels et des chercheurs doivent permettre d'imposer sa régulation. En France, l'histoire du RGPD date de quarante ans. Elle a débuté par la loi « informatique et libertés » grâce à des chercheurs qui ont étudié, testé, implanté, modifié. Au départ, la loi visait à se protéger de l'administration. La directive européenne y a ajouté la protection contre les entreprises. Cette histoire est longue, un secteur ne peut être régulé du jour au lendemain.

La puissance normative est importante, mais l'enjeu sera également de mettre fin à l'escalade des textes prétendant être d'application extraterritoriale. Certes, protéger nos citoyens passe par la revendication de l'application extraterritoriale de notre cadre juridique. Mais l'application extraterritoriale semble aujourd'hui instrumentalisée et l'incertitude juridique est croissante. Décréter l'application extraterritoriale d'un texte pour régler les problèmes n'est pas la panacée. Nous n'avons pas été les premiers à agir ainsi, mais ce n'est pas une excuse.

J'y ai fait allusion en début d'intervention, la plupart de nos start-ups produisent des applications pour smartphones. Elles doivent donc accepter les conditions générales d'utilisation et les data d'une demi-douzaine d'acteurs dont Facebook Connect, Paypal ou Google Maps. Finalement, la quasi-totalité de l'économie numérique est fondée sur des ressources que nous ne contrôlons pas.

La situation qui en découle est une situation de dépendance et de servilité. Nous devons faire face à cet enjeu. Bien sûr, une stratégie industrielle est nécessaire, à taille européenne, même si l'histoire ne plaide pas en faveur de cette idée. Malheureusement, chaque réponse européenne prend finalement la forme d'une quinzaine de réponses et le consensus sur une entreprise ou un pays est difficile à trouver. La France pourra peut-être démontrer sa solidarité européenne dans le cadre de la bataille de la 5G, en soutenant des entreprises par exemple suédoises. Afin d'éviter que la situation ne se répète dans dix ans, des réflexions peuvent déjà être engagées sur la 6G, le *cloud*, l'informatique quantique ou l'intelligence artificielle. Par le passé, nous avons raté des occasions et nous devons en tirer des enseignements. L'économie numérique est caractérisée par le phénomène du *winner takes all*. Donc partir deuxième pour imiter le premier est déjà partir perdant. L'innovation numérique ne fonctionne pas ainsi. Le projet Gaïa-X (infrastructure européenne de données) me semble basé sur des prémices différentes, avec une construction d'interopérabilité et de synergies (et non un « acteur champion » sur décision étatique). La stratégie industrielle nous offre encore de belles opportunités.

Si l'autonomie des ressources sur lesquelles nous innovons impose une industrie européenne, des actions peuvent aussi être menées avec les communs numériques (*Digital Commons*), des logiciels libres tels que Open Street Map ou Wikipédia. Travailler sur des données libres est le meilleur moyen de garantir que ces données resteront accessibles. Cette position doit être une composante de la stratégie de souveraineté, afin de ne pas s'affaiblir. De plus, cet enjeu relève également de l'aide au développement. En effet, certains pays lorsqu'ils construisent leurs infrastructures hésitent entre une offre chinoise ou Facebook. Nous aimerions leur conseiller de construire un socle en *open source* avec une net-neutralité dont ils seront garants de l'indépendance. L'AFD commence à financer des partenariats publics pour favoriser l'émergence de communs dans les pays.

Pour conclure et avant d'échanger, je reviens sur les notions de souveraineté nationale et de souveraineté européenne. Historiquement, la France était méfiante, privilégiant la souveraineté nationale. Des voix fédéralistes plaidaient pour une Europe fédérale. Ce débat est politique, mais, opérationnellement, sur certains sujets tels que la cybersécurité, nous pouvons décider d'une troisième voie consistant à mieux travailler ensemble. En effet, la cybersécurité de l'Europe se fonde sur des agences solides dans différents pays et qui coopèrent très bien. Elles échangent des informations et savent quand c'est nécessaire déclencher des sanctions à l'échelon européen ou des réglementations renforçant la sécurité globale telle que la directive NIS (*Network and Information System Security*). Ces actions ne sont pas contradictoires, mais elles impliquent de changer les modes de fonctionnement. Le sujet de la souveraineté numérique permet d'évoquer la souveraineté interopérable. L'Allemagne ou les Pays-Bas souhaitent une souveraineté puissante et disposent d'agences fortes. Nous pouvons prévoir des critères communs très concrets, comme une échelle de gravité des attaques, afin de nous comprendre immédiatement. Ainsi, en fluidifiant les interactions, une puissance européenne peut se construire sans transfert de souveraineté. De nombreux sujets que nous avons évoqués nécessitent une coalition européenne pour faire poids au niveau mondial. La France a clairement un rôle leader. Le Président de la République organise le mois prochain à Paris le Forum de Paris sur la Paix (*Paris Peace forum*) et le sommet *Tech for Good* qui réuniront de grands patrons et de grands penseurs de la Tech. Nous sommes leaders, mais notre puissance de négociation découle de notre position européenne.

J'espère avoir répondu à vos questions et je suis à votre disposition pour échanger.

M. le président Jean-Luc Warsmann. Je vous remercie monsieur Verdier pour cette intervention tout à fait intéressante.

Je souhaitais vous relancer sur le sujet de l'extraterritorialité. Vous avez évoqué deux approches, une extraterritorialité pour des principes de base et un principe de comportement national avec des législations extraterritoriales. Cette seconde approche ne pacifie pas les relations internationales. Pourriez-vous approfondir ce point ou bien nous produire une contribution écrite dans les semaines à venir sur ce sujet qui est au cœur de nos problématiques ?

M. Henri Verdier, ambassadeur pour le numérique. Je produirai un écrit, car il me semble difficile d'approfondir ce sujet aujourd'hui au sein de cette mission. Je précise que la protection de nos citoyens, *via* le RGPD, ne vise pas que les entreprises européennes. Les libertés fondamentales de nos citoyens sont à protéger de toutes pratiques y compris issues d'un État ou d'une entreprise extraeuropéenne. La France est claire sur ce point. Néanmoins, nous avons constaté des abus de décisions extraterritoriales venant d'autres continents. Certaines nous sont même apparues comme des violations de notre souveraineté. Nous considérons que quiconque souhaite accéder à des données en Europe doit passer par l'État et non se servir dans les infrastructures européennes, et ce quel que soit le bien-fondé de son objectif. Nous maintiendrons fermement cette position. Mais il semble que certains textes soient interprétables et des pays s'adjugent ce droit notamment pour lutter contre le terrorisme ou la criminalité. Cette attitude n'est pas justifiable, car une coopération judiciaire peut être mobilisée. Aujourd'hui, dans de nombreuses enceintes se brandit facilement la menace d'application de mesures extraterritoriales. Cela peut parfois paraître légitime et fondé, mais nous devons dire à nos partenaires que faire une loi nationale et la décréter extraterritoriale ne peut être qu'un dernier recours, peu à même de régler les querelles. Nous tâcherons d'approfondir ce sujet et je solliciterai notre direction des affaires juridiques qui enrichira ces réflexions.

M. Philippe Latombe, rapporteur. J'aurais deux questions. La première est générale. Parmi nos collègues parlementaires (incluant le Congrès et le Sénat américains), nous observons les prémices d'une volonté de démanteler les géants du numérique présents sur leur territoire. Quelle est la position de la France et de l'Europe ? Sommes-nous plutôt favorables à un tel démantèlement ? Ou bien la complexité de l'action pousse-t-elle plutôt vers d'autres solutions telles que l'interopérabilité ? Vous l'avez évoqué, pouvoir porter ces données permettrait de se passer de ces entreprises. Comment se positionnent la France et l'Europe ? La seconde question est la suivante. L'application du RGPD a été un porte-étendard côté européen, mais la Cour de justice de l'Union européenne nous a rappelés à l'ordre à deux reprises avec l'invalidation du *Privacy Shield* et la confirmation de la jurisprudence *Tele2* la semaine passée. J'aimerais que nous revenions sur le *Digital Services Act* (DSA). Comment le mettre très clairement en place et éviter les incertitudes juridiques systématiques ? Quelle est la position de la France et son influence dans l'écriture du DSA ?

M. Henri Verdier, ambassadeur pour le numérique. La France et l'Europe n'ont pas de positions sur le futur de telle ou telle entreprise. Le contraire serait étonnant puisqu'une décision de démantèlement implique la justice et se fonde sur des fondements sérieux. En revanche, nous souhaitons éviter les abus de position dominante qui empêchent l'innovation. J'avais répondu à une entreprise de l'innovation numérique qui se plaignait que nous souhaitions justement d'autres entreprises de ce type, et non qu'elle soit en situation de monopole. Aujourd'hui, une réflexion complexe, largement portée par le ministère de l'économie et des finances, porte sur ces acteurs systémiques (*gate keepers)* qui déterminent lourdement les dimensions économiques et politiques. Les outils anciens caractérisant une position dominante ne sont plus toujours pertinents. Par exemple, une position dominante dans le numérique peut venir de la possession d'un standard ou d'une donnée pivot incontournable.

Pour répondre à votre deuxième question, à l'intérieur du DSA nous interrogeons la régulation *ex ante* des plateformes à effet structurant. Le texte est européen, la France a apporté sa contribution à l'élaboration du texte et participera à sa transposition en trilatéral devant le Parlement. J'espère que nous serons tous capables, y compris le Parlement français, de soutenir les thèses défendues auprès de nos partenaires. En tant que responsable de la politique d'*open data*, j'ai vu de beaux textes, insuffisamment servis par le pouvoir de conviction de l'administration. Encore aujourd'hui, certains éléments suscitent de l'insatisfaction, mais cela pousse à avancer. Entre l'élaboration de textes clairs et leur application, un délai existe qui me semble normal. Le droit engendre un cycle judiciaire, fait de jurisprudence et d'approfondissements. Dans un monde idéal, tous s'aligneraient immédiatement sur un nouveau texte.

Mme Marietta Karamanli. Je vous remercie, monsieur l'ambassadeur, pour les éléments abordés. Je partage votre avis sur l'importance de la jurisprudence, essentielle en droit. Elle permet de bousculer et d'avancer. Vous avez évoqué le transfert des données personnelles entre l'Union européenne et les États-Unis. En juillet dernier, l'Union européenne a invalidé ce type de transfert en exigeant que les responsables du traitement des données évaluent eux-mêmes le niveau de protection des données dans le pays du destinataire. Pourriez-vous nous en dire plus sur les discussions sur ce sujet au niveau européen ? Il existe des mesures transitoires urgentes pour sécuriser l'activité des entreprises françaises et européennes dans ce domaine. Comment sécuriser aujourd'hui les transferts des données entre l'Union européenne et les États-Unis notamment au regard du transfert ultérieur des données des pays à des pays tiers ? J'avais souligné cette problématique dans un précédent rapport sur le sujet (datant de mai 2016), mais la crise sanitaire actuelle y ajoute un caractère d'urgence.

M. Henri Verdier, ambassadeur pour le numérique. Je ne saurais vous dire. Il faudrait poser la question à la direction générale des Entreprises (DGE) dont vous avez reçu le directeur. La Cour des comptes n'a pas interdit le transfert de données vers les États-Unis. Elle a fait tomber un régime de protection automatique et elle a rappelé qu'il appartenait à l'entreprise exportant les données de s'assurer qu'elle puisse garantir le respect et la protection de la vie privée. L'exportation de données n'a pas été interdite. La Cour a jugé en référence au droit, sans préjuger des conséquences. Des plans de prolongation de l'activité sont à déterminer. Toutefois, j'ai l'impression que certaines entreprises crient au loup plus fortement qu'il n'est nécessaire. Un grand réseau social a par exemple annoncé le risque d'une fermeture de son activité en Europe. Je pense pour ma part qu'ils vont rapidement trouver une solution adéquate.

Mme Laure de La Raudière. Je me demande si l'enjeu consistant à préserver un internet global face à des internets régionaux est réaliste. En effet, la Chine n'a pas d'internet global, mais son propre internet. Les États-Unis, en interdisant TikTok, livrent une réponse à l'internet régional de la Chine et, de toute façon, les Américains dominent le marché internet hors Chine. Quel est le bilan coûts-bénéfices de la doctrine d'un internet global ? Avec des internets régionaux, l'Europe pourrait appliquer clairement ses lois au niveau européen et établir des accords de coopération au niveau international. Je suis volontairement un peu provocatrice, car vous avez dit : « Il faut tout faire pour garder un internet global. »

M. Henri Verdier, ambassadeur pour le numérique. Je n'ai pas dit « tout faire », car mon carnet de chèques ne me le permet pas. Préconiser un internet libre, ouvert et unifié est une position clairement française. La fragmentation d'internet risque d'entraver la liberté d'expression, de limiter la compréhension mutuelle entre les peuples et de faire perdre des points de croissance mondiale. Mais allons un peu plus loin. Comme je vous l'ai dit, j'ai créé

ma première entreprise en 1985. À l'époque, les ingénieurs de France Télécom ne croyaient pas en internet et pensaient que son coût serait démesuré.

À titre personnel, je considère que la *Permissionless Innvoation,* grâce à un réseau ouvert et décentralisé a donné lieu à l'incroyable cycle d'innovations que nous avons connu. Elle a également permis l'émergence de réseaux sociaux et de géants qui ne sont pas internet. En effet, Facebook, Twitter ou TikTok consistent à entrer dans un espace privé avec un droit privé (régi par les conditions générales d'utilisation) et un design qui n'est pas basé sur la neutralité, la transparence ou la traçabilité. Au contraire, leur design est conçu selon le *business model* de l'économie de l'attention pour donner à voir aux utilisateurs des contenus et des publicités personnalisés visant à augmenter les revenus de l'entreprise. Un internet libre et ouvert ne contrevient pas à l'inspiration initiale des pères fondateurs. Il permet l'émergence d'acteurs dont il faut bien sûr réguler l'activité, mais qui démontrent le bien-fondé des principes fondamentaux.

Avons-nous une chance de gagner la partie ? Tout dépend du sujet. Internet comprend sept couches techniques différentes (les plus connus sont le protocole TCP/IP et le web). Je pense que cette base peut être conservée. Aujourd'hui, l'entreprise Huawei propose à l'Union internationale des télécommunications un nouveau protocole pour les TCP/IP. Certains pays ne l'accepteront jamais. Une autre bataille concerne la muraille dont s'entourent certains pays. Ils demandent ainsi à leurs opérateurs d'aller sur un DNS (*Domain Name System*) national qu'ils filtrent pour supprimer ce qui ne leur convient pas. Néanmoins, quelqu'un de débrouillard, muni d'un réseau virtuel privé (*Virtual Private Network*-VPN), pourra tout de même accéder à l'internet mondial. La censure instaurée concerne donc les masses, elle n'est pas définitive. Ensuite, dans les couches très hautes, des applications peuvent-elles être bannies ? L'Inde (et bientôt les États-Unis) a banni TikTok de l'App store. Les Indiens qui avaient TikTok l'ont toujours, mais de nouveaux téléchargements sont désormais impossibles. Cela peut faire partie d'une stratégie de négociation. Il n'y aura pas d'internet similaire partout avec les mêmes lois. Des stratégies de conflictualité et de protectionnisme vont se développer. L'essence et le cœur doivent être préservés et dans ce domaine, la bataille n'est pas perdue.

M. Pierre-Alain Raphan. Vous l'avez rappelé, le développement de la pratique de la donnée de l'intelligence artificielle devient une stratégie de domination des États dans les différentes régions du monde. Je m'interroge sur les impacts sur la démocratie au sens large et notamment la manière de s'informer. Les récents scandales, notamment celui de Cambridge Analytica, ont montré l'impact sur les libertés individuelles. En effet, l'*open data* est une stratégie très intéressante pour la protection des données en France et en Europe. Mais se pose la question des pratiques individuelles. Votre fonction d'ambassadeur du numérique implique-t-elle des relations fortes avec les ministères chargés de la jeunesse et des sports, le ministère de l'enseignement supérieur, voire le service national universel ? En effet, il me paraît important de mettre en place des programmes d'acculturation sur les grands enjeux du numérique et de diffuser des messages pour mieux se protéger individuellement de cette potentielle fuite de données via les smartphones (les géolocalisations sont quasi imposées) et des réseaux sociaux. L'interaction entre ministères permet-elle aujourd'hui une acculturation populaire sur ces sujets ?

M. Henri Verdier, ambassadeur pour le numérique. Je précise que je ne suis pas ambassadeur du numérique, mais ambassadeur, au sein du ministère des affaires étrangères, pour les affaires numériques. Je suis en charge des négociations internationales et de la politique extérieure de la France pour les affaires numériques. Je m'occupe moins fondamentalement de la politique nationale. Vous avez raison, la liberté individuelle, la démocratie et la souveraineté sont interdépendantes. La souveraineté et la démocratie sont nécessaires pour protéger la liberté individuelle et la liberté individuelle est nécessaire pour

protéger la démocratie et affirmer sa souveraineté. Cette interdépendance est sans doute nouvelle pour le numérique. Mais cela ne relève pas des attributions de l'ambassadeur pour les affaires numériques.

M. Philippe Latombe, rapporteur. Je vous soumets une dernière question que nous n'avons pas encore totalement abordée. Elle porte sur la taxation et la fiscalité des géants du numérique. Les négociations autour de la « taxe GAFA » échouent, sont relancées, échouent à nouveau. Que pouvez-vous nous en dire aujourd'hui ? Où en sommes-nous et quelles suites sont à donner ? Quelle est la position de la France à ce sujet et quels échos existent chez ses partenaires européens ? Je rappelle que la Cour de justice de l'Union européenne avait annulé une amende d'Apple.

M. Henri Verdier, ambassadeur pour le numérique. Ce sujet est en effet encore assez douloureux, car un dumping fiscal demeure entre les pays européens. La vraie question n'est pas une taxe GAFA. D'ailleurs, le ministre de l'économie et des finances a annoncé hier qu'il exercerait son droit de la prélever pour l'année 2020 puisque les négociations à l'OCDE n'avancent pas. La vraie question est celle d'une fiscalité numérique. Depuis des siècles, l'imaginaire fiscal considère que la valeur est prélevée sur le site de production, soit l'usine où se trouvent les salariés, avec une propriété intellectuelle provenant du bureau d'études de l'entreprise. Or, dans le numérique, la valeur relève du consommateur qui utilise le produit, reçoit la publicité, partage ses données et crée encore plus de valeur. Nous devons apprendre à prélever la valeur auprès des utilisateurs plutôt qu'auprès de la création. D'autant que certaines entreprises prétendent que cette création est tout entière de la propriété intellectuelle laquelle est tout entière localisée aux Bahamas. La fluidité numérique permet d'abuser de cette différence.

Depuis longtemps, la France porte ce sujet *via* le rapport « Colin-Collin », l'avis du Conseil national du numérique, les tentatives de portage à l'OCDE… Aujourd'hui, un groupe de travail constitué de représentants de cent vingt pays traite de ce sujet. La France ne vise pas une fiscalité des acteurs du numérique, mais une fiscalité du numérique, compatible avec l'économie numérique. Ce point est crucial. À défaut de prendre la valeur là où elle se crée, la base fiscale s'effrite et les acteurs en mauvaise santé sont affaiblis. Continuer à fiscaliser les perdants sans fiscaliser les gagnants revient à faire de la pression fiscale un handicap. Nous continuerons et nous finirons par l'emporter, car nous avons raison. Mais lors de telles négociations, chacun fait ses comptes. Les pays qui hébergent les géants du numérique ne sont ainsi pas favorables à une telle taxe. La France, souveraine, a donc décidé une taxe GAFA en attendant mieux. Cette taxe GAFA a été annoncée, puis suspendue dans l'attente de l'issue des négociations au sein de l'OCDE. Hier, Bruno Le Maire a annoncé l'échec de ce round des négociations et l'instauration d'un prélèvement de la taxe GAFA pour 2020. La taxe GAFA n'est pas la finalité. L'enjeu est que les systèmes fiscaux soient cohérents avec l'économie réelle actuelle.

Audition, ouverte à la presse, de M. Cédric O, secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques
(22 octobre 2020)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Monsieur le ministre, je vous remercie d'être présent et vous salue au nom du président la mission Jean-Luc Warsmann, présent à distance au téléphone, ainsi qu'en mon nom.

Nous poursuivons donc nos travaux avec l'audition de M. Cédric O, secrétaire d'État en charge de la transition numérique et des communications électroniques. Nous vous entendons, monsieur le ministre, sur la souveraineté numérique qui est au cœur de nos préoccupations et de votre périmètre d'action. Elle regroupe en effet des questions larges, qui vont du déploiement d'infrastructures numériques autonomes dans notre pays à la régulation des plateformes en passant par le soutien aux acteurs du numérique et par les enjeux de cybersécurité. Il nous semble important, dans le cadre de notre mission, que vous nous fassiez connaître vos orientations sur ces différents sujets et les positions portées au niveau européen par la France.

La souveraineté numérique est une thématique particulièrement riche. Nous essaierons de l'aborder de la manière la plus large possible, de nombreux sujets étant porteurs d'enjeux indispensables à sa construction, qu'elle soit française ou européenne. Il est ainsi difficile de parler de souveraineté numérique sans évoquer d'abord le rôle des grandes plateformes qui occupent une place essentielle dans l'économie numérique. Leur régulation a déjà fait l'objet de débats au sein de l'Assemblée nationale. La Commission européenne travaille actuellement sur un *Digital Services Act* qui traite à la fois la responsabilité des plateformes numériques pour le contenu qu'elles hébergent et les problèmes suscités par leur rôle de *gatekeepers* – contrôleurs de l'accès des utilisateurs – ayant la charge des écosystèmes de plus en plus importants desdites plateformes. Celles-ci vont jusqu'à aborder le sujet de la monnaie virtuelle avec le lancement par Facebook du projet Libra. Nous souhaiterions, monsieur le ministre, avoir votre éclairage sur l'ensemble de ces sujets.

La souveraineté numérique comporte également une dimension technologique puisque le développement de nouvelles technologies s'organise autour de la possession et de la maîtrise des données. Les modalités de soutien à notre écosystème d'entreprises dites de la « tech » mais aussi la protection des données personnelles sont deux sujets sur lesquels nous aimerions également vous entendre.

Je n'oublie pas le plan de relance qui comporte une forte dimension numérique et technologique. Vous pourrez peut-être nous en dire un mot.

Enfin, il est important de rappeler que la souveraineté numérique ne peut être séparée des enjeux de cybersécurité des infrastructures. Nous aimerions connaître votre vision sur ce que doit être la cybersécurité française et nous souhaiterions faire avec vous un point d'étape sur la 5G. Les enchères viennent de s'achever pour la bande de 3,5 GHz et les déploiements commerciaux devraient débuter à la fin de l'année 2020. La mise en œuvre d'un régime d'autorisation spécifique vis-à-vis de ces équipements témoigne de la nécessaire vigilance

stratégique qui doit accompagner des déploiements par ailleurs fortement utiles pour notre économie.

M. Cédric O, secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques. Le sujet nécessiterait peut-être quatre ou cinq auditions pour être traité dans le détail. Il n'a échappé ni à cette mission ni, maintenant, à l'ensemble des Français, que la souveraineté numérique est désormais au cœur des questions de souveraineté nationale, qu'il s'agisse des questions de souveraineté économique ou de souveraineté politique.

Nous l'avons vu pendant le confinement, les outils ayant permis de rendre le confinement plus acceptable, plus supportable, étaient très souvent des outils anglo-saxons. Nous nous rendons dramatiquement compte – avec les évènements de la semaine dernière – que certaines infrastructures numériques essentielles, presque aussi importantes que les ponts, les réseaux d'eau, le réseau téléphonique ou les routes, sont des infrastructures privées – ce qui n'est pas forcément un sujet en tant que tel – sur lesquelles l'État et les institutions publiques ont peu de capacité de régulation dans le cadre juridique actuel. Elles sont quasiment toutes anglo-saxonnes. Les alternatives européennes peuvent exister mais ont de toute évidence une empreinte économique et démocratique bien moindre.

Vous avez évoqué la régulation des grandes plateformes. C'est, je pense, l'un de deux piliers absolument essentiels de la question de la souveraineté numérique mais ce n'est pas le plus important. Le plus important est notre capacité à maîtriser ces technologies et à avoir des acteurs économiques capables de concurrencer les grands acteurs américains et chinois.

Je prends quelques exemples dans des secteurs clés que sont l'intelligence artificielle (IA) et le *cloud*. D'après les chiffres de 2017, les Américains investissent chaque année 40 milliards de dollars dans l'IA, tandis que les grandes plateformes chinoises et le gouvernement chinois investissent chaque année 40 milliards d'euros. Les chiffres sont similaires en ce qui concerne le *cloud*. Les investissements des entreprises européennes dans ces deux domaines, qui sont absolument stratégiques pour notre souveraineté, ne dépassent pas 4 milliards d'euros.

L'entreprise Apple, à elle seule, vaut quant à elle actuellement plus que l'ensemble du CAC 40. Dans quelques semaines, ce sera aussi vrai pour Microsoft. L'émergence de ces géants leur donne une puissance financière, une puissance d'investissement et d'acquisition, qui est sans commune mesure avec ce que les entreprises européennes et les États européens sont capables de faire. Nous pouvons considérer que ces entreprises sont trop grosses. C'est probablement le cas mais, même si elles valaient dix fois moins, elles conserveraient des valorisations et des capacités d'investissement inatteignables aujourd'hui pour les Européens.

L'âge moyen des entreprises du CAC 40 est supérieur à cent ans. L'âge moyen de leurs homologues anglo-saxonnes est inférieur à vingt ans et, pour les Chinois, il doit être inférieur à dix ans. Les deux dernières introductions en bourse d'une entreprise technologique française de plus d'un milliard d'euros – soit environ 1 500 fois moins qu'Amazon ou Apple – sont Dassault Systèmes en 1996 et Worldline.

L'équation économique est très simple : soit nous sommes capables de faire émerger des entreprises dont la puissance est aussi forte que celle des Américains et des Chinois, soit toute notion de souveraineté numérique est absolument illusoire. La régulation ne suffira pas à tout résoudre. Diminuer la taille ou démanteler ne changera pas le fait que ceux qui ont les produits et qui investissent sont les Américains et les Chinois.

Il ne faut certes pas avoir une vision binaire du sujet. L'écosystème de la French Tech se développe. Nous avons des investisseurs, des entrepreneurs, des entreprises extraordinaires. Cet écosystème devient actuellement le premier de l'Union européenne, ce qui est très encourageant. Cependant, la question économique reste centrale. Nous n'aurons pas de souveraineté technologique si nous ne sommes pas capables de créer les conditions financières adaptées, au sens des conditions fiscales, du marché du travail, des conditions de fiscalité individuelle.

C'est encore plus vrai dans une situation où les citoyens européens sont schizophrènes. Le consommateur adore ces grands groupes même en détestant leur comportement fiscal, éthique… Il « vote avec ses pieds » mais plébiscite le service qu'ils rendent. Si ce n'était pas vrai, Facebook n'aurait pas le monopole des réseaux sociaux, Amazon n'aurait pas une telle empreinte sur le commerce en ligne, Google n'aurait pas le monopole des moteurs de recherche. La raison est simple ; ces groupes sont en effet extrêmement forts en termes de consumérisme. Le premier élément pour faire émerger des entreprises capables de concurrencer les entreprises anglo-saxonnes s'appuie dès lors sur l'investissement, l'environnement fiscal et l'environnement du marché du travail.

Chaque année, 5 milliards d'euros sont investis dans les start-up françaises et plus de 100 milliards dans les start-up américaines. Je n'ai pas le chiffre européen mais il est largement inférieur au chiffre américain. Il existe actuellement environ 450 « licornes » – des entreprises valorisées à plus d'un milliard d'euros – dont environ 200 aux États-Unis, 200 en Chine et 30 en Europe.

Nous n'avons pas d'autre choix que de développer un écosystème numérique à la hauteur des enjeux, justifiant que le Président de la République, le Premier ministre et moi-même y consacrons autant de temps et d'investissements, notamment dans le cadre du plan de relance. L'horizon indépassable de notre souveraineté numérique est d'avoir les acteurs capables de la réaliser, au-delà des décisions sectorielles dans le domaine des jeunes entreprises disruptives – « Deep Tech » –, de la cybersécurité ou des biotechnologies. C'est au cœur de ce que veut faire la Commission européenne, avec des montants d'investissements extrêmement importants, au cœur de la politique du Gouvernement. Nous devons avoir cette dimension offensive car la dimension de la régulation ne suffit pas.

Le deuxième pied sur lequel nous devons avancer est la régulation, d'un point de vue souverain sans doute mais aussi démocratique et économique. Aux États-Unis et en Chine, des acteurs économiques dont l'empreinte sur notre économie et notre démocratie est difficilement soutenable ont émergé. C'est vrai dans le domaine économique avec des comportements prédateurs et monopolistiques ou oligopolistiques. C'est vrai dans le domaine démocratique comme les évènements récents nous l'ont démontré.

Dans ce cadre, la régulation de ces acteurs est une question internationale qui se pose en France évidemment mais en Europe de façon plus générale et aussi aux États-Unis. Je suis allé aux États-Unis à la fin de l'année dernière ; la question de la puissance de ces acteurs et de leur empreinte est centrale dans l'équilibre démocratique des États-Unis eux-mêmes. Nous verrons ce qu'il se passera en fonction du résultat des élections américaines mais la régulation de ces acteurs nous semble aujourd'hui indispensable. C'est ce que la France porte de manière extrêmement forte dans le *Digital Services Act* qui doit être présenté par la Commission européenne début décembre.

Les deux éléments principaux sont : la nécessité de la mise à jour de nos règles de concurrence pour faire en sorte que nous les adaptions à la question de l'économie numérique et des modèles d'affaires des grands acteurs du numérique ; la nécessité de mettre en place

une régulation spécifique de ce que nous appelons les plateformes structurantes, c'est-à-dire les plateformes qui ont une empreinte telle dans un secteur ou sur une économie qu'elles deviennent des *gatekeepers*, des gardiens de l'accès. Ces plateformes étant quasiment devenues des infrastructures essentielles, elles doivent se voir appliquer une régulation *ex ante* qui soit à la hauteur de l'enjeu tout comme nous avons régulé les réseaux d'eau, les réseaux téléphoniques, les réseaux routiers… Je pense aux réseaux sociaux, aux terminaux mobiles, aux moteurs de recherche. Il nous faut un régulateur à la hauteur de cette ambition.

Si nous voulons recouvrer notre souveraineté politique sur ce domaine à la croisée du politique et de l'économique, nous devons avancer sur ces deux points : être au bon niveau économique et avoir des acteurs que nous régulons ici même.

Il est important d'avoir des acteurs que nous régulons ici, pour une raison simple : je suis persuadé que les entreprises ont une identité et une nationalité. Lorsque vous êtes sur une plateforme ou un réseau social américain, vous êtes régulé par des conditions générales d'utilisation d'inspiration anglo-saxonne. Vous êtes soumis à une entreprise dont l'identité est profondément anglo-saxonne même si elle s'adapte évidemment de temps en temps au pays dans lequel elle opère. Une entreprise dont le siège social et le patron sont américains est différente d'une entreprise dont le siège social et le patron ou la patronne sont européens par leur culture, par leur approche de la question des valeurs de l'entreprise et par la capacité d'influence des états. Cette question de la régulation dépasse l'aspect national. Elle me semble être une question démocratique. Nous avons donc à la fois une question économique offensive et une question de régulation plus défensive.

Le *Digital Services Act* est un horizon extrêmement important et décisif pour les dix ans qui viennent. Soit l'Europe est à la hauteur de l'enjeu, soit nous aurons laissé passer une occasion absolument décisive. Les premières propositions mises sur la table par la Commission européenne sont extrêmement intéressantes et positives, je dois le dire. Nous savons toutefois qu'il peut arriver qu'elles s'effilochent avec le temps. J'ai rappelé au Conseil « Télécommunications » de la semaine dernière que nous sommes vigilants pour maintenir ce niveau d'ambition. Nous sommes sur ce sujet alignés avec la plupart des pays européens, notamment avec l'Allemagne ou les Pays-Bas avec lesquels j'ai cosigné un document sur la régulation.

Vous avez évoqué la cybersécurité qui est évidemment au cœur de la souveraineté numérique. Nous devons être très forts en cybersécurité mais ce n'est pas indépendant de la question économique. La cybersécurité demande de l'intelligence artificielle, de la maîtrise du *cloud*… Si nos acteurs ne sont pas parmi les meilleurs du monde dans l'intelligence artificielle et la maîtrise du *cloud*, nous serons en retard en matière de cybersécurité. Il ne suffit pas de financer les spécialistes du *cloud* ou de l'intelligence artificielle ; Facebook n'a notamment rien d'une entreprise profondément technologique à l'origine, c'est un réseau social. Toutefois, cette entreprise a tellement grossi, est devenue tellement monopolistique qu'elle vaut maintenant 700 milliards de dollars et est capable d'investir des dizaines de milliards de dollars.

L'État n'a pas à choisir entre une entreprise de cybersécurité, une entreprise de livraison de repas et une entreprise de réseau social pour l'investissement et la croissance de l'écosystème économique parce que c'est peut-être une entreprise de réseau social qui, demain, grossira et aura une capacité d'investissement telle qu'elle deviendra un acteur majeur de l'intelligence artificielle.

Nous considérons la question de la cybersécurité comme critique. Nous avons dans le cadre du plan de relance décidé que la cybersécurité serait particulièrement traitée parmi les

marchés critiques. C'est un sujet sur lequel la France, comme dans tous les domaines de la souveraineté, a la volonté d'être autonome.

Je rappelle que la France est dans le monde occidental, à part les États-Unis, le seul pays qui s'attache à maîtriser l'ensemble de composantes de la souveraineté stratégique. Cela va de la question nucléaire à la cybersécurité offensive et défensive où la France est attachée à ne dépendre d'aucun pays, que ce soit pour ses capacités de renseignement ou pour ses capacités défensives d'attribution et de contrôle de ce qu'il se passe sur ses réseaux par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cette agence est considérée comme dans le top 5 ou 6 des agences ayant un savoir-faire en matière de cybersécurité.

Nous avons besoin, en plus de ce savoir-faire reconnu par les entreprises et nos homologues européens, de développer un écosystème privé d'entreprises de la cybersécurité. Nous avons plusieurs acteurs de taille internationale, notamment dans les très grandes entreprises françaises comme Orange, Thalès, Atos, Airbus, Capgemini, que ce soit dans la production de matériel ou de logiciels. Nous avons un écosystème très performant de start-up, de petites et moyennes entreprises et d'entreprises de taille intermédiaire (PME et ETI). Nous souhaitons consolider ce savoir-faire pour maîtriser l'ensemble des chaînons technologiques de la cybersécurité. Nous avons vu à travers le développement des attaques informatiques des institutions, des entreprises ou même des citoyens, à quel point cette maîtrise est importante.

M. Philippe Latombe, rapporteur. Vous avez dit qu'il faut investir dans le *cloud* et ne pas laisser les États-Unis notamment prendre la tête. Nous avons interrogé voici quelques semaines les représentants des fabricants de composants électroniques. Ils nous ont dit que nous avions très clairement perdu le match sur le *cloud* et sur l'intelligence artificielle dans le *cloud* et qu'il fallait que la France se spécialise. D'après eux, la France a de bonnes capacités notamment dans l'intelligence artificielle décentralisée, l'industrie automobile étant un bon exemple de ce savoir-faire. La meilleure solution est, à leur avis, que nous nous spécialisions dans ce domaine. Vous nous disiez pourtant que vous vouliez absolument que nous investissions dans le *cloud*.

Par ailleurs, nous n'avons pas abordé la question de l'organisation de l'État. Nous voyons que l'État souhaite numériser l'ensemble de son fonctionnement mais le fait ministère par ministère. Pourquoi, à l'instar d'autres pays, n'avons-nous pas un ministère dédié au numérique, qui soit transversal, donc relié directement au Premier ministre ? Cela existe à Monaco et dans d'autres pays européens. Le numérique ne peut pas se voir simplement ministère par ministère, en silos. Il doit irriguer la totalité du fonctionnement de l'État.

Enfin, nous avons beaucoup entendu parler de la plateforme des données de santé (*Health Data Hub*, HDH) et du recours à Microsoft. La question des marchés publics se pose et il faut voir comment privilégier des solutions européennes dans le cadre des marchés publics. Qu'en pensez-vous ? Le code des marchés publics affirme très clairement certaines impossibilités alors que la souveraineté passe aussi par la maîtrise des lieux de stockage des données. Une réflexion est-elle en cours pour savoir comment privilégier des acteurs français ou européens dans les marchés publics français ou européens ?

M. Cédric O, secrétaire d'État. Je ne pense pas que nous ayons perdu le match du *cloud* ou de l'intelligence artificielle. Nous avons perdu les deux premiers sets. La question fait certes débat et est l'objet de discussions répétées avec les industriels du secteur, clients et fournisseurs. La France et l'Europe ont-elles perdu le match du *cloud* et de l'intelligence artificielle ? Cela vaut-il encore le coup de le mener ? Ma conviction est que oui, cela vaut le

coup. Je constate qu'une partie de l'écosystème estime le contraire, compte tenu des montants en jeu.

Les deux sujets sont un peu différents. Sur la question du *cloud*, nous avons perdu les deux premiers sets sur des scores très sévères. Je pense que le match peut encore être joué mais que cela nécessite des investissements et une volonté constante, au bon niveau, pour développer nos acteurs. Même ainsi, ce n'est pas certain que nous réussissions.

Je considère en revanche que nous avons, pour longtemps, perdu le match de l'intelligence artificielle appliquée aux données personnelles et aux consommateurs. Les bases de données constituées par les très grandes entreprises américaines ou chinoises, exponentiellement grandissantes, font que l'écart s'accroît chaque jour.

Il existe des domaines dans lesquels nous pouvons toutefois encore jouer, et même dans lesquels nous pouvons être parmi les meilleurs du monde. Cela concerne notamment les données industrielles et l'intelligence artificielle appliquée à certains secteurs du commerce interentreprises (*B to B*), tels que les domaines de la santé, des transports, de l'environnement, de l'énergie, de la cybersécurité. Partout où le savoir-faire français est extrêmement fort, avec des très grandes entreprises françaises et des lacs de données à la bonne taille, nous sommes capables de créer des savoir-faire parmi les meilleurs du monde parce que nous avons l'une des meilleures écoles du monde en mathématiques et en informatique.

Pour faire le lien avec le HDH, la création de l'entrepôt des données de santé a été décidée parce que nous avons un très fort savoir-faire en France en intelligence artificielle et sur la question médicale. Notre pays est particulièrement centralisé en termes de données médicales, ce qui est un avantage compétitif très important. Les bases de données françaises de l'Assistance publique-Hôpitaux de Paris (AP-HP) et de l'assurance maladie sont parmi les cinq plus grosses bases de données de santé du monde. Nous avons donc intérêt, pour des raisons médicales et économiques, à connecter l'ensemble de ces bases de données afin de découvrir des interactions médicamenteuses, faire de la recherche, du suivi individualisé de patients, améliorer la qualité des soins, améliorer la vie des personnels de santé et faire émerger des champions français de la santé numérique ou développer le savoir-faire de nos entreprises.

Le HDH n'est qu'une surcouche. Les données de santé des Français ne sont, à 99 %, pas dans le HDH aujourd'hui. Elles sont stockées dans les *data centers* des différents hôpitaux, des laboratoires qui sont pour la plupart hébergés chez des Français. Nous avons voulu créer une surcouche qui, tout en respectant un processus extrêmement normé sur les questions de données personnelles et d'éthique, permette de connecter les données nécessaires pour faire fonctionner des algorithmes d'intelligence artificielle. L'objectif est de créer des champions de la santé numérique et d'améliorer la santé des Français.

Cette décision a été prise dans le cadre de la présentation par le Président dela République du plan sur l'intelligence artificielle en mars 2018. Elle a donné lieu à la consultation de dix-neuf entreprises sur l'outil mis à la disposition du HDH. La seule entreprise qui répondait début 2019 aux critères techniques de performance, de capacité à développer ces algorithmes, était Microsoft. Il a alors été décidé de démarrer tout de suite avec Microsoft une phase expérimentale de développement, parce que cette société était en avance dans le domaine de l'intelligence artificielle. D'ailleurs, si vous discutez aujourd'hui avec les entreprises de l'intelligence artificielle, elles vous feront toutes part de l'extrême avance des groupes américains.

Notre volonté est de faire émerger des champions européens capables de tenir tête à Microsoft Azure, à Google Cloud ou à Amazon Web Services (AWS). C'est bien sûr

indispensable mais, à ce moment et sur cette question de la santé, Microsoft était le plus avancé. Il a donc été décidé de débuter avec lui une période probatoire. Nous avons pu ainsi, pendant la crise de la covid du début d'année, faire des découvertes extrêmement intéressantes sur des interactions médicamenteuses ou des facteurs de comorbidité. Très concrètement, si nous avions dû attendre un an ou un an et demi pour travailler avec un acteur français, nous ne l'aurions pas fait pendant la crise de la covid parce que nous n'aurions pas été prêts.

Voici donc la situation objective. J'ai toutefois été très clair lors d'une audition au Sénat. Notre volonté est de faire passer le HDH sur une infrastructure européenne, notamment pour une raison juridique. En effet, une décision de la Cour de justice de l'Union européenne a estimé juridiquement impossible que le HDH continue à être hébergé sur des infrastructures américaines à terme, le Conseil d'État ayant par ailleurs considéré qu'il n'y avait pas urgence. Notre volonté est donc de travailler à la transition vers une infrastructure européenne. En conséquence, nous devons être capables de mettre à jour nos capacités de traitement algorithmique. Dans le cas inverse, ce que nous aurons gagné en indépendance industrielle sera perdu en opportunités sanitaires. Juridiquement, les données étaient suffisamment protégées compte tenu des clauses contractuelles. Passer le HDH sur des infrastructures européennes n'est donc pas anodin.

Encore une fois, Amazon avec AWS investit 22 milliards de dollars par an en recherche et développement. La France tout entière investit un peu plus de 60 milliards par an dans l'ensemble de sa recherche. Sans géant du web européen, nous n'aurons pas de solution. Notre conviction est que nous devons faire en sorte que ces géants émergent, que ce soit dans le *cloud*, dans l'intelligence artificielle… mais cela prendra du temps. La Silicon Valley s'est créée à la fin des années 1950. Même si cela ne prend pas autant de temps, il en faut pour faire émerger ces acteurs. En ce qui concerne le HDH, la décision est claire ; il passera, dans les mois ou les années qui viennent, sur une infrastructure européenne.

Vous m'avez interrogé sur la possibilité de privilégier des solutions européennes. Je rappelle que la législation européenne, sauf pour ce qui concerne la défense nationale, ne nous permet pas de faire de différence entre une entreprise américaine ayant un siège en Europe et une entreprise européenne ayant un siège en Europe. Elles sont juridiquement à traiter de la même manière. Il existe une petite différence dans le cas du *cloud* : compte tenu de la législation extraterritoriale prise par les États-Unis, nous estimons que toutes les conditions juridiques de sécurité des données ne peuvent être remplies. C'est d'ailleurs le cœur de la décision de la Cour de justice de l'Union européenne sur l'affaire *Schrems II* et l'invalidation du « *Privacy Shield* ». Pour les questions qui relèvent au sens large de la souveraineté mais qui n'en relèvent pas au sens juridique, il n'est pas possible de faire une différence entre une entreprise américaine et une entreprise européenne. La décision n'est pas à la main de l'État français, même si nous pouvons le regretter.

Je ne suis pas le mieux placé pour répondre à la question d'un ministère dédié au numérique. Je pense que le fond du sujet est de faire progresser la culture de l'État, des hauts fonctionnaires et des ministres sur les questions du numérique et de l'importance du numérique. Nous avons vu encore la semaine dernière, de façon dramatique, à quel point le numérique irrigue l'ensemble de notre vie quotidienne et de nos politiques publiques. Il répond à des codes qui ne sont pas exactement les mêmes que ceux de la vie réelle, à certaines contraintes et opportunités. Il est important que chaque politique publique soit conçue dans une approche notamment numérique, pas uniquement tout de même, et de faire en sorte que nos politiques soient décidées de manière holistique en prenant en compte le numérique.

Sera-ce mieux avec un ministre d'État du numérique ou faut-il que chaque ministre injecte du numérique dans sa politique publique ? Encore une fois, je ne suis pas le mieux

placé pour y répondre. Cela me rappelle les débats dans les entreprises privées pour savoir s'il faut une direction de la transformation numérique du groupe ou s'il faut injecter du numérique dans chaque unité commerciale. Les choix peuvent évoluer d'ailleurs. Il pourrait y avoir un intérêt symbolique à le faire mais le principal est de faire en sorte que le numérique progresse au sein du Gouvernement et des administrations.

À cet égard, je considère que ce Gouvernement et cette majorité ont fait progresser d'un pas inédit la question du numérique. Est-ce suffisant ? Probablement pas. Devons-nous continuer ? C'est certain. En tout cas, le numérique a, au sein de ce gouvernement, une place qu'il n'avait pas dans les gouvernements précédents. Ayant fait partie de ceux-ci, je le sais et je pense que, en la matière, le plus intéressant est d'écouter la manière dont les entreprises du numérique en parlent. Nous ne sommes certainement pas au bout du chemin.

M. Philippe Latombe, rapporteur. Vous avez parlé de l'arrêt de la Cour de justice de l'Union européenne dans l'affaire *Schrems II*. Le niveau européen est important. Il a construit le règlement général de protection des données (RGPD). En lien avec la Cour de justice de l'Union, il a par ailleurs fait *Schrems II* et a confirmé *Tele2*. Vous avez par ailleurs évoqué le *Digital Services Act*. Pouvez-vous revenir sur les points que la France souhaite voir intégrés dans ce projet de directive ? Quelles avancées proposées par l'Europe vous conviennent-elles et pourraient créer des ruptures ou permettre des innovations ?

M. Cédric O, secrétaire d'État. Dans le cadre du *Digital Services Act*, la France porte trois éléments particuliers. Le premier concerne la régulation économique des plateformes, le deuxième la régulation des contenus et le troisième la régulation du commerce en ligne.

La question de la régulation économique des plateformes est probablement ce qui fait le plus consensus au niveau européen. La position de la France est simple. Certaines entreprises sont aujourd'hui en position monopolistique ou oligopolistique. Leur empreinte sur notre économie et notre société a atteint un point tel qu'elles doivent se voir appliquer une régulation asymétrique, extrêmement forte et qui leur soit dédiée. L'actualisation de nos outils de concurrence ainsi que la mise en place de régulations et de supervisions dédiées avec un superviseur de niveau européen dédié sont donc indispensables. Il pourrait imposer des notions d'interopérabilité et de régulation d'accès à certains services, les terminaux par exemple, considérés comme des infrastructures essentielles pour lesquelles nous ne pouvons pas laisser s'exercer la libre concurrence. Il pourrait aussi imposer des notions de transparence sur les pratiques de ces plateformes. Nous ne savons actuellement pas comment elles se comportent exactement. Le régulateur pouvait imposer des obligations pour contrôler les secteurs et marchés dominés par ces plateformes, en les considérant comme des infrastructures essentielles.

Nous n'écartons pas la question du démantèlement et nous souhaitons qu'elle reste sur la table, comme l'a demandé la France de manière précise. Le démantèlement est toutefois un ultime recours. En effet, d'abord, concrètement, il prendrait vingt ans compte tenu des recours juridiques ; ensuite il n'est pas certain que cette solution soit la plus efficace. Les modèles économiques sont changeants.

J'ai d'ailleurs eu une très intéressante discussion avec l'ancien président de la *Federal Communications Commission* (FCC), équivalent aux États-Unis de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Sa position était : « *Don't break them up, break them open* » – ne pas les briser, mais les ouvrir – donc de passer par l'interopérabilité, l'ouverture des données et la régulation. Il estimait que ce serait beaucoup plus efficace et rapide. Il faut toutefois garder le démantèlement dans la boucle des sanctions, où il existe déjà.

Il convient par ailleurs d'éviter certaines fusions qui nous semblent dommageables, comme l'acquisition d'Instagram ou de WhatsApp par Facebook. Elles conduiraient non seulement à empêcher la concurrence mais à renforcer la situation monopolistique des acteurs.

Compte tenu de ce que la Commission européenne a posé sur la table avec la mise à jour des règles de concurrence et le *Digital Services Act*, je crois que le terrain est favorable pour progresser sur ces questions en Europe. Nous le verrons début décembre.

Les obligations de modération de contenu appliquées aux plateformes font plus débat. Cette question relève moins de la souveraineté numérique mais davantage malheureusement de l'actualité. Aujourd'hui, les grands réseaux sociaux sont régis par la directive « e-commerce » sur le commerce électronique qui les rend irresponsables des contenus publiés sur leurs plateformes car ils ne sont pas éditeurs mais simplement hébergeurs.

La France soutient qu'il faut considérer, à l'image de la deuxième partie de la « loi Avia » visant à lutter contre les contenus haineux sur internet, la nécessité d'obligation de moyens pour les plateformes dans la modération et la régulation des contenus les plus problématiques. La loi a été invalidée par le Conseil constitutionnel, mais seulement par voie de conséquence en ce qui concerne cette deuxième partie, donc sans jugement au fond.

Les plateformes devraient se doter d'équipes de modération à la hauteur de l'enjeu qu'elles représentent. Facebook et Twitter n'ont ainsi pas le même. Elles doivent avoir des obligations de moyens sous la supervision d'un régulateur. La France est extrêmement offensive sur cette question. Il nous semble qu'il s'agit d'un bon équilibre entre la régulation et la liberté d'expression.

Ce sujet fait en Europe infiniment plus débat que la question économique pour des raisons de sensibilités culturelles à la liberté d'expression, qui sont assez différentes. Certains pays européens ne souhaitent rien ajouter à la régulation actuelle des plateformes. La capacité de notre pays à réguler cette question est incertaine, étant sous directive européenne. Nous sentons les lignes bouger et nous poussons en faveur cette obligation de moyens.

Ces obligations de moyens seraient fixées au niveau européen, avec éventuellement une supervision européenne, mais la définition des contenus illicites ne relève évidemment pas d'une définition européenne. La culture française n'est pas la même que la culture suédoise ou la culture portugaise sur la liberté d'expression et la haine en ligne. Nous souhaitons donc que des obligations de moyens soient posées au niveau européen tandis que la définition des contenus illicites resterait à la main des États, compte tenu des forts liens avec les héritages culturels.

Nous portons enfin la question de la régulation des places de marché. Certaines, comme Wish que j'ai eu l'occasion de dénoncer en tant que ministre pendant le confinement, ont des comportements vis-à-vis de leurs vendeurs qui sont d'une irresponsabilité totale. Vous trouvez aujourd'hui sur certaines places de marché une majorité d'articles vendus par des vendeurs non européens et non conformes aux règles européennes. Dans la régulation actuelle, ces plateformes sont irresponsables, au sens qu'elles ne sont pas responsables juridiquement. Vous pouvez, sur ces plateformes, acheter un jouet qui explosera à la figure de votre enfant sans que la plateforme soit redevable de quoi que ce soit. C'est inacceptable.

La France porte le fait que des obligations spécifiques soient imposées aux places de marché sur le contrôle de la conformité de leurs vendeurs non européens, pour s'assurer que les vendeurs non européens respectent les mêmes règles que les vendeurs européens et ne soient pas irresponsables. C'est une question qui dépasse la liberté d'expression et relève de

la sécurité sanitaire. L'Europe serait fondée à être beaucoup plus dure et à sortir du cadre de la directive « e-commerce » sur ce sujet spécifique.

Voici donc les trois positions que la France porte dans le cadre de la nouvelle directive sur les services numériques.

M. Pierre-Alain Raphan. Je souhaite évoquer l'aspect de la souveraineté mais de l'autre côté de la barrière. Je me suis basé sur un très bon livre de Joël de Rosnay, intitulé *Je cherche à comprendre*, qui parle d'internet et de ses impacts sociétaux. Il dit qu'internet est une sorte de gros corps dont l'ADN est l'humain, puisque nous alimentons en permanence ces sujets par nos propres données. Il n'est pas difficile de dire que la crédulité de l'humain est plus facile à corriger que la puissance de la technologie alliée au capitalisme.

Vous avez rappelé la nécessité absolue d'acculturation des citoyens et des politiques en premier lieu. Tous sont également manipulés au quotidien par les *dark patterns* qui alimentent cette économie de l'attention. Ne pourrions-nous pas réfléchir collectivement à un grand programme national d'acculturation, à la formation de chacun à l'économie de l'attention et au numérique au sens large ? Pourquoi ne pas organiser un débat national ou une convention citoyenne sur le numérique ?

Nous devons faire des choix qui ne soient pas que des choix d'experts mais aussi des choix de citoyens. De très nombreux sujets doivent être posés sur la table et débattus collectivement, comme la reconnaissance faciale.

S'agissant de la modération, est-il envisagé de travailler avec les plateformes ou les médias sociaux sur l'instantanéité des messages ? Ainsi, sur Twitter ou Facebook, lorsque je poste un message, il part tout de suite mais nous savons très bien, comme le fait Google par exemple, qu'il peut exister un petit contrôle. Par exemple, si j'écris « vous trouverez en pièce jointe… », que j'oublie la pièce jointe et que j'appuie sur « Envoyer », Google signale que j'ai oublié d'envoyer la pièce jointe. Un contrôle se fait donc. Avec les moyens dont nous disposons, nous pouvons reconnaître automatiquement, avec quelques erreurs certes, des images ou des phrases à caractère très violent, des insultes ou des incitations à la haine. L'algorithme pourrait dire dans ce cas : « Êtes-vous bien sûr de vouloir envoyer ce message, sachant que vous pouvez vous exposer à une amende, de la prison, au transfert de votre adresse IP aux autorités… ? » avec un rappel à la loi.

Ainsi, nous ne toucherions pas à la liberté des citoyens de dire ce qu'ils veulent mais ce micro-contrôle permettrait de réfléchir et de ne pas s'embarquer dans une ivresse collective qui amène aux actes les plus odieux.

M. Cédric O, secrétaire d'État. Je vous rejoins totalement sur votre premier point, monsieur le député. Les dérives des acteurs d'internet sont largement liées à l'ignorance de nombre de nos concitoyens – et même des responsables politiques évidemment – de la manière dont cela fonctionne et des sous-jacents d'un monde de plus en plus numérique.

L'inclusion numérique me semble absolument essentielle si nous voulons continuer à faire société dans le cadre de citoyens autonomes et émancipés. Nous savons qu'un Français sur six n'utilise jamais d'ordinateur. Un Français sur trois manque de compétences numériques de base. L'inclusion numérique commence par apprendre à créer une adresse e-mail, à déclarer ses impôts en ligne, à vendre un objet sur « Le Bon Coin » ou à faire un WhatsApp avec des proches pour une personne isolée.

Dans une session de médiation numérique où les citoyens apprennent à devenir autonomes, les questions qui suivent l'explication de la création d'une adresse e-mail portent sur les données personnelles, les fausses informations, la parentalité à l'heure du numérique, les écrans. Le sujet porte certes sur des capacités très concrètes mais le fond est un sujet de grammaire, de compréhension par nos concitoyens de cette grammaire du monde numérique.

Je conseille assez largement la lecture du sociologue Gérald Bronner : le numérique a tendance à favoriser les instincts anciens, les explications unifactorielles par rapport à des explications multifactorielles. Nous apprécions le fonctionnement en silos informationnels favorisé par le numérique.

La seule manière de combattre les nombreuses dérives du numérique, sur les fausses informations, sur la haine en ligne ou sur la puissance des grandes entreprises d'internet, est de former nos concitoyens. Il faut les faire progresser et progresser nous-mêmes car nos concitoyens ne sont pas les seuls à être en retard. Les serviteurs de l'État, les hauts fonctionnaires, ne sont guère en reste. Je pense que nous ne sommes actuellement pas au bon niveau. Il faut que nous accélérions sur ce sujet.

Avons-nous besoin d'une convention citoyenne sur le numérique ? Pourquoi pas, mais je pense que les prochaines échéances empêchent ou compliquent la tenue de ce genre de cénacle. Toutefois, nous avons besoin d'une réflexion sociétale sur la question du numérique, sans le saucissonner entre données, géants du web (GAFA), haine en ligne, inclusion numérique et question économique.

Dans la perspective de la nomination du prochain Conseil national du numérique puisque l'ancien a terminé ses travaux cet été, nous voulons justement mettre sur la table la question de cette capacité à avoir une approche multidisciplinaire et holistique de ce sujet essentiel du numérique.

Je pense que l'instantanéité de messages doit être une piste de travail. Cela ne résoudra évidemment pas tout mais, dans le cadre des obligations de moyens et de modération, elle est une des solutions. Il faut ralentir le caractère viral de certains contenus, particulièrement des plus offensants. Nous sommes au cœur du modèle d'affaires des plateformes et de l'économie de l'attention. Les contenus qui retiennent le plus votre attention, ceux que vous aurez le plus tendance à commenter ou à partager, sont les contenus les plus choquants ou les plus agressifs. Ce sont donc les plus rémunérateurs puisqu'ils font le plus de vues.

En appelant à l'émancipation et à l'autonomie individuelle, certains éléments pourraient effectivement conduire des personnes à se demander : « Ai-je vraiment besoin de dire cela, de partager ce contenu ? » Je pense que c'est une très bonne question et un outil sur lequel nous devons travailler, une forme de modération *ex ante* qui n'irait pas jusqu'au bout.

Nous devons aussi avoir conscience, particulièrement dans le cadre des évènements de la semaine dernière, que la modération des contenus n'est pas humainement possible. Il faudra qu'une part importante des décisions soit prise par des algorithmes. Cela pose des questions de transparence des algorithmes, de redevabilité de ceux qui les font, qui les déploient… Le sujet est complexe mais je suis assez favorable à votre proposition pour certains acteurs dont l'empreinte est telle qu'ils sont devenus peut-être la première agora publique. Cette question pourrait être étudiée en France, d'autant plus que ces acteurs utilisent déjà en partie ces algorithmes. Ainsi, lorsque vous postez votre message, il peut être retiré dans la seconde qui suit. L'intérêt de votre proposition est que cette modération se fasse en amont et j'y suis plutôt favorable.

M. Philippe Latombe, rapporteur. Je reviens sur la formation. Le code est aujourd'hui absolument nécessaire dans l'écosystème. Le code est un langage, une langue étrangère. Pensez-vous que son apprentissage, non pas dans le supérieur mais dès le plus jeune âge, est actuellement suffisant à l'école ? Devrions-nous le développer ? Sans ces futurs codeurs et donc l'acculturation au code par les plus jeunes, nous n'y arriverons pas. Pensez-vous que la France a une vraie spécialité dans le code ? Nous avons des codeurs de très haut niveau mais nous avons tendance à les laisser partir ensuite.

Ne serait-ce pas également un moyen d'avoir un équilibre entre les garçons et les filles pour avoir ensuite des étudiants et des étudiantes dans les écoles d'informatique et les écoles d'ingénieurs spécialisées dans le numérique ?

Quelle vision portez-vous, en tant que secrétaire d'État mais aussi dans le Gouvernement ? Je rappelle que le langage Python est étudié au lycée. D'autres langages sont en train de sortir comme le langage Julia qui est une invention française. Nous avons OCaml, nous avons une spécificité française. Avons-nous suffisamment de formation et d'acculturation au langage pour conserver cet avantage ?

M. Cédric O, secrétaire d'État. La question est du ressort du ministre de l'éducation, Jean-Michel Blanquer, mais j'ai évidemment un avis. Oui, nous devons faire progresser nos jeunes sur la question du code. C'est le cas dans le monde entier. Il ne s'agit pas véritablement de la question du code mais de ce qu'il induit de compréhension des mécanismes numériques et de compréhension de la grammaire de notre monde. Personnellement, je ne code pas mais j'ai quelques petites connaissances qui me permettent de mieux comprendre ce qui est faisable ou infaisable. Nous avons donc besoin d'augmenter le niveau de nos élèves. La question de cette nouvelle « langue étrangère » et même de plusieurs langues étrangères est un problème mondial.

Nous devrions évidemment faire plus, aller plus vite mais, au regard de ce qui a été enclenché par l'éducation nationale au niveau national, la France est aujourd'hui l'un des pays qui fait le plus d'efforts pour éduquer ses élèves au code. La modification introduite par la réforme du lycée et du baccalauréat fait que, en seconde, tous les élèves ont chaque semaine une heure et demie d'enseignement technique et numérique. La France est le premier pays à avoir généralisé cet enseignement en seconde.

Il existe certes des endroits, aux États-Unis ou dans d'autres pays, où certaines écoles sont plus en avance sur l'enseignement du code mais la France est le seul pays de l'Organisation de coopération et de développement économiques (OCDE) à avoir généralisé cet enseignement. Il est inscrit dans une feuille de route ambitieuse qui commence en primaire et se poursuit au collège puis au lycée.

Des difficultés de transition se posent, notamment celle du professorat puisqu'il faut former des professeurs. Jean-Michel Blanquer me disait, voici quelques mois, que l'éducation nationale avait été extrêmement surprise par l'enthousiasme et l'adhésion des professeurs de lycée, notamment les professeurs de technologie, pour se faire former à cette question de l'éducation numérique.

Nous devons aller plus loin. L'éducation nationale a, je pense, à cœur de faire progresser ce sujet et de progresser vite. C'est d'autant plus important qu'il faut que nous essayions progressivement de descendre sur le collège et même sur le primaire, où d'ailleurs des modules d'initiation sont déjà prévus. Cette question est aussi liée à la mixité et à l'égalité femmes-hommes puisque le déport des petites filles sur la question de l'enseignement numérique commence assez tôt, dès le primaire, et se cristallise au moment du collège, lorsque

des choix d'orientation sont faits en quatrième et troisième. Il faut aller plus loin et pas que pour apprendre à développer des jeux vidéo. Il s'agit de comprendre le monde dans lequel nous évoluons.

S'agissant des codeurs qui s'en vont, je pense d'abord que qu'ils sont moins nombreux actuellement. Nous assistons, depuis un ou deux ans, avec une accélération depuis six mois, à un mouvement de retour des Français entrepreneurs ou développeurs partis à l'étranger. Je n'ai pas encore de chiffres mais ce mouvement est très intéressant. L'attractivité de l'écosystème français pour des entrepreneurs, des salariés, des développeurs étrangers, est plus élevée qu'elle ne l'a jamais été. Elle est probablement liée au climat américain actuel, au Brexit mais aussi à l'augmentation de la maturité de l'écosystème français et à l'image de la France, de son Gouvernement, de son écosystème numérique sur les start-up.

Si nous voulons que nos codeurs et développeurs restent, ils doivent pouvoir disposer d'entreprises dans lesquelles ils s'épanouiront autant qu'aux États-Unis. C'est le cas aujourd'hui et le sera de plus en plus.

Dans le fond, je suis très optimiste sur cette question de la souveraineté numérique et de l'écosystème numérique ; en effet, je pense que la compétition mondiale pour la technologie est d'abord une compétition mondiale pour l'intelligence humaine. Or la France a cette intelligence humaine. Elle forme des ingénieurs, des chercheurs et des entrepreneurs parmi les meilleurs du monde. Il s'agit juste de les garder et qu'ils trouvent ici l'écosystème leur permettant de développer des entreprises qui seront demain parmi les meilleures du monde. Cela prendra un peu de temps mais elles y arriveront. La dynamique actuellement observée, pour des raisons fiscales aussi, est très encourageante.

Mme Valéria Faure-Muntian. Je pense qu'il est urgent de rendre obligatoire à l'école primaire, vers six ou sept ans, l'apprentissage du codage. Au-delà, puisque nous sommes forts en France sur les systèmes de données comme nous le voyons avec le système de santé, nous devrions être innovants sur la partie apprentissage des données de manière très pédagogique. Je pense que c'est très urgent.

Il ne faut pas oublier l'outil *Computer Science For All* initié par le précédent Président des États-Unis. Les enfants, dès la sortie de la maternelle, avaient des cours dans ce domaine. Ils n'étaient évidemment pas obligatoires puisqu'aux États-Unis le système n'est pas national. Le fait que nous ayons un système harmonisé nationalement en France peut faciliter cet apprentissage.

J'ai également une question concernant les identifiants numériques, un sujet sur lequel nous n'évoluons pas. Cette identification permettrait d'harmoniser les échanges interministériels ainsi que les échanges entre tous les systèmes. Je ne sais pas où nous en sommes. Des rapports sont faits. Quelle suite y est-elle donnée ? Quels sont les freins identifiés ?

Concernant la santé numérique pour laquelle nous avons une force liée à notre système de sécurité sociale nationale, le risque de l'entente avec Microsoft est évidemment que des sociétés récupèrent un certain nombre de données. Je suppose que tout ceci est bien « bordé ». Ces données sont tout de même la plus grande richesse, plus que les algorithmes me semble-t-il. Nous pouvons essayer d'avancer, de développer des algorithmes, en revanche les données sont une richesse sans prix. Pourriez-vous donner quelques informations complémentaires sur l'accord conclu ?

Enfin, nous avions dès le début de la mandature des relations avec l'Estonie. Où en sommes-nous ?

M. Cédric O, secrétaire d'État. Je crois que le secrétaire d'État chargé de la transition numérique est assez favorable au code obligatoire à l'école mais je vous invite à évoquer ce sujet avec le ministre de l'éducation. Je ne veux pas nous opposer.

Nous aimerions effectivement aller plus vite mais je pense que ce qui a été fait depuis le début du quinquennat par Jean-Michel Blanquer est absolument remarquable. Il faut probablement aller plus loin encore mais aucun pays de l'OCDE n'a fait ce que fait la France sur l'enseignement obligatoire du code dès le lycée. Il s'agit maintenant de descendre vers les niveaux inférieurs et je partage votre avis.

Sur l'identifiant numérique, le premier problème est celui de l'identifiant numérique unique des Français par les administrations puisqu'il est interdit par la Commission nationale de l'informatique et des libertés (CNIL). Le moteur et la clé de la réussite estonienne sont l'identifiant unique puisqu'il s'agit de communiquer entre les administrations. Toutefois, le Conseil d'État, au moment de la discussion sur le numéro de sécurité sociale, qui est en fait le seul identifiant, a estimé que l'usage de cet identifiant devait rester proportionné et qu'il n'était pas possible d'avoir un identifiant unique de l'administration.

Cela n'empêche pas que nous progressons assez vite sur la question de l'échange d'informations entre les administrations dans le cadre du programme « Dites le nous une fois ». Je vous invite à auditionner ma collègue Amélie de Montchalin qui pilote la transformation numérique de l'État. L'identité numérique des Français doit commencer à être déployée l'été prochain.

En ce qui concerne le contrat passé avec Microsoft, je n'ai pas d'inquiétude sur la récupération commerciale des données. Les entreprises n'y ont pas intérêt et les clauses juridiques sont très protectrices. Le cryptage des données n'est pas assuré par Microsoft mais par les Français. La question posée par le *Cloud Act* et le déploiement du HDH sur l'infrastructure Microsoft est plutôt la question de l'extraterritorialité des décisions américaines et de la capacité des Américains, dans le cadre de décisions judiciaires, à avoir accès aux données des Français en se passant de l'autorisation de l'entreprise et de l'autorisation des autorités françaises.

Ce n'est pas un problème de diffusion des données des Français aux acteurs américains ; cela n'arrivera pas. Le problème est la défense de la souveraineté de données des Français. Des échanges d'informations entre les justices se font dans le cadre d'une entraide judiciaire et non le cadre d'une décision unilatérale de la justice américaine. Pour cette raison, la Cour de justice de l'Union européenne a estimé que le *Cloud Act* ne permettait pas à des entreprises américaines de traiter des données européennes. C'est aussi la raison, compte tenu de la forte sécurité juridique, qui a conduit le Conseil d'État à considérer que la migration du HDH n'est pas urgente, en tout cas que la décision prise n'est pas illégale, même si la CNIL a été très claire sur la nécessité d'opérer une transition.

Nous avons évidemment des échanges avec l'Estonie. J'admire beaucoup le système estonien qui a l'avantage de ne pas avoir été bâti sur une administration datant de plusieurs centaines d'années et ayant ses propres processus. Nous devons tendre vers cette facilité d'usage pour les citoyens en priorité. La question de l'identité numérique est un point clé et j'espère que la mise à disposition de cette identité l'été prochain permettra de faire des progrès importants.

Mme Marion Lenne. Je reviens sur le code à l'école. Je pense que ce sont vraiment les usages qui font que quelqu'un s'intéresse au code. Aujourd'hui, le numérique est au cœur de la pédagogie et tous les enfants, même les filles, veulent l'apprendre. Ma petite dernière regarde ses devoirs en ligne lorsqu'elle rentre à la maison et, si je lui dis qu'elle peut se créer son propre jeu, elle s'intéressera au code. Ce sont les usages qui créent l'intérêt, pas l'éducation nationale. C'est le moment d'y aller parce que les usages sont là.

Le statut du télétravailleur frontalier n'a, quant à lui, aucun sens. En effet, il dépend de la caisse de son pays d'emploi sauf s'il reste chez lui et dépasse 25 % de son temps de travail dans son pays de résidence. Je suis allée à Berne la semaine dernière pour voir le représentant de l'Union européenne et lui dire qu'il faut travailler sur ce sujet. C'est un non-sens en fait. Nous travaillons aujourd'hui où nous voulons, quand nous voulons et les frontières n'existent plus dans la vie des travailleurs. Comment l'institution peut-elle se mettre à la page de la réalité citoyenne ? Il m'a été répondu que c'est aux entreprises de jouer le jeu, ce qui sera difficile à expliquer aux citoyens. Il reste un gros travail à faire sur ce sujet.

M. Cédric O, secrétaire d'État. Je vous rejoins volontiers sur le fait que le développement du télétravail et d'entreprises, de start-up qui considèrent comme possible de travailler à 100 % en télétravail d'où que ce soit dans le monde repose très sensiblement les questions du droit du travail et des fiscalités individuelles et collectives. Il se pose toutefois la question de la soutenabilité d'un tel modèle, y compris pour les entreprises elles-mêmes compte tenu des difficultés à intégrer les nouveaux et à avoir un attachement à l'entreprise. Ce problème se pose déjà pour les travailleurs frontaliers. La question d'une communauté de vie démocratique et fiscale se posera encore plus si une part importante des Français travaille depuis la France pour des entreprises étrangères et vice-versa. Il faut repenser un certain nombre de cadres, peut-être parfois de façon expérimentale.

Je n'ai pas la réponse compte tenu des questions essentielles qui sont posées mais je vous rejoins sur la nécessité d'y réfléchir. Je rappelle que le télétravail semble parfois être pour certains employeurs une nouvelle manière pour les employés de moins travailler, tandis que, pour certains syndicats, c'est le nouveau vecteur privilégié de la prolétarisation du travail. Je pense que le télétravail est quand même en règle générale très bien vécu par les employeurs et les employés, particulièrement lors de crise telle que celle de la covid. Cela ne signifie pas qu'il ne faut pas de règles.

Nous avons tout intérêt à favoriser le télétravail dans cette crise et, même à terme, il est probable que l'équilibre entre travail physique et travail digital soit repositionné. Ce sera très bien compte tenu de ce qu'il apporte pour la vie personnelle et la productivité.

M. Philippe Latombe, rapporteur. J'ai une question sur le 5G. Sans rentrer dans les polémiques sur les ondes, la 5G a posé et continue de poser une question de matériel. Une décision américaine a été prise de limiter le recours à un fabricant de matériel chinois, Huawei.

Quelle est aujourd'hui notre dépendance à ce matériel ? Sommes-nous capables de déployer la 5G selon le plan prévu avec du matériel européen ? La position quasi monopolistique de Huawei nous avait fait nous poser des questions et, depuis, des évolutions ont eu lieu. Comment voyez-vous la situation, sachant que le matériel a été autorisé sous conditions, pendant un temps limité ?

Quelles sont donc les perspectives, uniquement sur la partie matérielle ?

M. Cédric O, secrétaire d'État. Sur la question du matériel et des équipements 5G, la position de la France est extrêmement claire. Elle a toute légitimité à prendre des décisions

qui garantissent sa souveraineté. Les appareils 5G ne posent pas un problème de captation de données personnelles mais peuvent poser, compte tenu de leurs caractéristiques techniques, un problème de résilience globale du système si un ou plusieurs équipementiers ont une empreinte énorme, ainsi qu'un problème d'accès à certaines données industrielles ou certaines données sensibles. Un équipement 5G n'a donc pas la même sensibilité selon qu'il se trouve à côté de l'île Longue ou dans la campagne en Rhône-Alpes.

C'est dans ce cadre qu'une proposition de loi a été votée à l'initiative du député Éric Bothorel. Elle a imposé que chaque équipement 5G fasse l'objet d'une validation par l'ANSSI et d'une décision du Premier ministre en fonction de la nature de l'équipement et de son lieu de déploiement. Nous estimons que ce cadre garantit de manière très efficace la souveraineté française.

J'apporte un amendement à ce que vous avez dit : il n'existe pas de monopole de tel ou tel fournisseur. Orange n'a sur le territoire hexagonal que des équipements européens, Free n'a quasiment que des équipements européens, SFR a un tiers d'équipements non européens je crois – je vérifierai – et de même pour Bouygues. De manière globale, l'empreinte des équipements non européens sur le territoire français est très limitée. La France est d'ailleurs l'un des pays européens où l'empreinte des fournisseurs non européens est la plus faible.

Nous avons décidé dans ce cadre que nous donnerons des agréments à l'ensemble des fournisseurs mais que, en fonction des caractéristiques des équipements et de leur position, nous donnerons ou non l'autorisation d'installer. Nous serons attentifs à l'endroit où ces antennes sont placées et à l'empreinte globale du fournisseur. Nous estimons que ces décisions sont nécessaires et suffisantes pour assurer la souveraineté française.

D'autres pays ont pris des décisions différentes, dans les deux sens, en donnant plus ou moins d'autorisations. Je leur laisse évidemment la latitude et la responsabilité de leur décision. Nous estimons quant à nous que la souveraineté n'est pas remise en question compte tenu des décisions prophylactiques qui ont été prises.

M. Philippe Latombe, rapporteur. Je vous remercie, monsieur le ministre.

Audition, ouverte à la presse, de Mme Geneviève Bouché, présidente du Forum Atena, et de MM. Éric Lemaire, président, et Wilfried Bartsch, ancien président de l'association pour la souveraineté numérique Opération Lancelot
(29 octobre 2020)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Le président Jean-Luc Warsmann est avec nous en audio. Je vais le remplacer pour le mot d'ouverture. Je suis très heureux de vous accueillir aujourd'hui, Mme Geneviève Bouché, présidente du forum Atena, MM. Wilfried Bartsch et Éric Lemaire, présidents ancien et actuel de l'association Opération Lancelot.

Notre mission d'information va, pendant plusieurs mois, se pencher sur les moyens de bâtir et de promouvoir une souveraineté numérique française et européenne. Il nous apparaît primordial de recueillir l'analyse d'acteurs au croisement des sphères publique et privée.

À cet effet, nous souhaiterions que vous nous présentiez en quelques mots vos organisations respectives afin de nous indiquer leur mode de fonctionnement, leurs activités et la façon dont elles s'engagent sur cette thématique.

Le thème de la souveraineté fait immédiatement appel au cœur régalien des missions de l'État, mais nous engage également à une réflexion sur les armes économiques dont nous devons disposer pour défendre la place de notre pays et de l'Union européenne dans la compétition mondiale. Sur ces deux plans, régalien et économique, nous aimerions connaître votre opinion sur la montée en puissance de la notion de souveraineté numérique. Comment l'analysez-vous ? Que pensez-vous des positions adoptées au niveau national et européen sur ces sujets par les autorités publiques ? Quelle appréciation portez-vous sur les initiatives législatives en cours ? Savez-vous si les parlements des autres États membres de l'Union ont des débats sur ces questions ?

La souveraineté numérique française ou européenne est confrontée à la montée en puissance de nouveaux acteurs privés qui prétendent imposer leurs normes et/ou qui disposent d'un pouvoir de marché les rendant bien souvent incontournables pour les consommateurs et les usagers. Comment la France et l'Union européenne peuvent-elles selon vous reprendre la main sur la définition des termes dans ces rapports nouveaux afin de ne pas être réduites à une position strictement réactive, voire passive ? Quelle pourrait être la contribution d'une politique de la concurrence nouvelle dans ce domaine ? Jugez-vous que nous pouvons encore gagner la bataille des normes ? Quelles sont vos analyses sur les premières annonces concernant le *Digital Services Act* qui sera présenté par la Commission européenne début décembre ?

Enfin, la défense de la souveraineté numérique passe aussi par une certaine autonomie matérielle et par la défense et la promotion d'une industrie du numérique européenne compétitive et indépendante. Or, nous savons que l'Europe souffre de façon croissante du départ d'industries stratégiques pour le matériel informatique qui constituent pourtant le soubassement du développement du numérique. La dépendance aux solutions technologiques extracommunautaires, aussi bien les logiciels que les matériels, met-elle en cause, selon vous, l'autonomie européenne ? Comment contrer cette tendance et comment faire participer l'innovation et la recherche à une certaine forme de réindustrialisation dans les nouvelles technologies à même d'assurer une plus grande souveraineté européenne ? Sur quels secteurs

et quelles technologies faut-il aujourd'hui, selon vous, miser ? À hauteur de quels moyens ? Comment le plan de relance européen peut-il être utilisé à cette fin ? Sur un plan plus régalien, quelle est votre perception des grands enjeux de la cybersécurité ? Comment la France et l'Union européenne pourraient-elles s'affirmer dans les domaines de la cyberdéfense ou de la certification de sécurité ? Quels sont selon vous nos atouts et nos faiblesses pour développer une véritable industrie européenne de la cybersécurité ?

Mme Geneviève Bouché, présidente du Forum Atena. Je suis présidente du Forum Atena, la deuxième présidente puisque ce *think tank* date de 2007. Les Français connaissent mal l'histoire du numérique français en raison d'une omerta très forte. Le temps commence à venir de raconter cette histoire. Pour moi, il s'agit quasiment d'une affaire de famille, puisque je suis la petite-fille de du mathématicien René Dontot qui a créé les mathématiques qui permettent de faire les univers 3D, et je suis la nièce de Jacques Dontot, dirigeant de Thomson CSF, qui a été entravé dans le développement du numérique, dirigeant qui a créé Sony France avec des laboratoires en France avec son ami Morita Akio, qui était le fondateur de Sony. La France et le Japon étaient pendant les années 1950, 1960 et 1970 très en pointe dans le numérique.

J'ai fait mes études à l'université de Paris-Dauphine, pour devenir ingénieure systèmes télécoms et en économie. Au niveau du troisième cycle, j'ai fait une spécialisation qui préparait aux fonctions de commissaire au plan et j'étais la « thésarde de service » qui était dans le périmètre de Simon Nora qui rédigeait alors le rapport Nora-Minc. Nous avions des réflexions sociétales extrêmement poussées, sur les relations entre numérique et société. Surtout, les liens entre numérique et géopolitique n'ont jamais cessé de me préoccuper.

Quand je suis arrivée à France Télécom, j'ai été en charge de développer le numérique français dans les couches hautes. J'ai dirigé une équipe d'ingénieurs qui a été brutalement coupée en deux en 1981 ou 1982 : la moitié est partie aux États-Unis et l'autre moitié a été dispersée en France. Cette coupure a été un traumatisme pour nous. Nous avons su ce qui nous était arrivé : l'on nous a expliqué que ce qui nous était arrivé n'était pas racontable, avec des moyens de pression assez forts.

J'en viens au sujet qui nous préoccupe aujourd'hui. Finalement, le savoir-faire n'a pas quitté le territoire. Nous sommes quand même assez nombreux. Que peut-on faire avec le numérique ? Sur ce sujet, la pensée française et européenne était absolument différente de la pensée américaine. Quand la moitié de mon équipe est partie aux États-Unis, mes archives sont aussi parties au MIT (*Massachusetts Institute of Technology*). Nous avons eu des échanges avec les Américains et nous avons tout de suite vu que nous n'avions pas du tout la même idée. Ils avaient une idée hégémonique, une idée de *soft power*, qui aujourd'hui montre ses limites.

Nous avions une idée complètement différente : rendre la France efficace. Les accords secrets qui faisaient que nous n'avons pas pu développer notre numérique à nous reposaient sur des idées très avant-gardistes. Nous voulions faire un numérique biomimétique ou symbiotique, c'est-à-dire très modulaire, « scalable » et interopérable. Nous partions du principe qu'un problème doit pouvoir être traité en interaction avec les autres et qu'il existe des variants et des invariants. Il faut faire un numérique qui est bien adapté à un certain endroit, un autre qui ressemble avec les invariants et qui s'adapte avec les variants d'un autre endroit et, de cette façon, l'on arrive à avoir un numérique en rhizome.

L'Europe a été entravée dans le développement de son propre secteur numérique. Les grands informaticiens ont en général des cursus scolaires chaotiques, car c'est quelque chose qui relève plus de la créativité, de la compréhension du monde que de la rationalité qui est

essentielle pour faire un bon parcours, rentrer dans les bonnes écoles, *etc*. Tous ces résilients de l'informatique qui font de l'informatique parce qu'ils y voient de l'esthétique, parce qu'ils y voient de l'enthousiasme, parce qu'ils y voient un espace où l'on peut changer le monde, se sont organisés à travers l'Europe.

L'Europe a la communauté *open source* la plus vivace du monde. Il s'agit d'un fonds de commerce extrêmement précieux pour l'Europe. L'Europe, c'est les premiers systèmes d'exploitation qui ont été repris par IBM, en contre-feu de la puissance de Microsoft, c'est Skype que vous connaissez, c'est tout ce qui a été fait dans le *peer-to-peer*. Toutes ces réalisations reflètent tout à fait la pensée du numérique européen qui est un numérique modulaire, « scalable » et interopérable. C'est notre mode de pensée, et cela tombe bien parce que l'Europe, sur le plan politique et géopolitique, est la zone géographique qui est en train d'inventer une forme de démocratie qui est régie par ces principes.

Aujourd'hui, nous avons en France tous les composants pour faire un numérique alternatif et pourtant compatible avec le numérique mondial. En matière de management de l'innovation, on explique à nos étudiants que, quand on a pour une raison quelconque raté une marche dans une évolution, courir après le leader est inutile, il est de loin préférable de se mettre à l'affût de la vague suivante, voire la susciter et, à ce moment-là, reprendre la main.

Le numérique qui nous est imposé, auquel vous avez fait allusion dans votre mot introductif, qui désigne assez fortement les GAFAM et les BATX, c'est pour nous le numérique 0.0. C'est un numérique qui est basé sur une chimère : devenir le maître du monde. Quand vous vous référez à la légende de Babel, vous savez que cette idée est mortifère. Ce 0.0 est centralisateur. Or la centralisation en informatique en particulier et en management de systèmes introduit forcément de la calcification. Ce numérique 0.0 n'est donc pas éternel. Il a été construit avec une grande rapidité (vingt ans pour les GAFAM et une dizaine d'années pour les Chinois). En matière de technologies, plus vive est l'ascension, plus vive est le retournement technologique. Quand nous nous adossons à ce numérique, nous prenons un risque.

Nous avons donc intérêt à nous mettre en *pole position* sur la vague qui arrive, sur un numérique modulaire, « scalable », *etc.* C'est ce qui se fait de fait, même sans avoir l'autorisation, c'est ce que ma corporation, celle des informaticiens, et en particulier les informaticiens systèmes et réseaux, ont fait. En France, nous avons des noyaux à portée de main. Vous avez toute la bibliothèque Framasoft dont on ne s'occupe pas ou tout à fait insuffisamment. Elle est d'ailleurs en ce moment en train de replier la toile, ce qui est dommage. Il faut vite voler à leur secours et leur donner la lumière dont ils ont besoin.

En matière de numérique, nous avons écouté attentivement l'audition de Cédric O. Je vous ai envoyé par écrit l'analyse que nous en faisons. Cédric O est très impressionné, puisqu'il a une culture un peu financière, par la capitalisation des acteurs du numérique américains et chinois. Il faut avoir une vision économique de la question. La richesse dont nous parlons est une richesse immatérielle. Une richesse immatérielle ne se comporte pas du tout comme une richesse matérielle. Quand vous vous servez d'une richesse matérielle, elle se déprécie alors que quand vous vous servez d'une richesse immatérielle, elle se bonifie.

Nous avons cette richesse immatérielle, nous avons le POC estonien qui est l'une des architectures système les plus abouties qui existent au monde. Il s'agit d'un modèle. Il existe du tourisme technologique en Estonie. Je suis vraiment admirative du travail qui a été fait avec des Français, des Danois, des Européens en général. Les Français se sont impliqués dans cette architecture qui est d'inspiration d'Europe du Nord. Les circonstances ont fait que nous ne

valorisons pas cette richesse immatérielle, mais elle est sur le territoire. Il suffit de se mettre d'accord sur le numérique que nous voulons.

En matière d'architecture réseau, nous préconisons une architecture appelée RINA (*Recursive InterNetwork Architecture*). RINA est basée sur le datagramme qui a été designé dans les années 70, mais qui a fait l'objet de recherches permanentes jusqu'à aujourd'hui. RINA est expérimentée en Arménie actuellement avec beaucoup de succès. Vous savez que l'internet se fragmente. Ce n'est pas la peine de lutter contre la fragmentation de l'internet. Je vous renvoie à la légende de la Tour de Babel pour comprendre ce que vit l'internet mondial.

Aujourd'hui, nous nous retrouvons dans une situation qui ressemble au Moyen Âge, mais dans le cyberspace. Au Moyen Âge, l'on a construit des châteaux forts pour protéger les richesses et les gens qui créent de la richesse en cas d'attaque. En matière de cybersécurité, nous préconisons d'avoir l'équivalent des châteaux forts qui nous permettent de protéger notre environnement et de gérer de façon séparée les indésirables internes et les indésirables externes. Le numérique que nous préconisons est un numérique qui n'a pas pour vocation de faire de l'autarcie numérique, car l'autarcie est mortifère. Dans la nature, une cellule qui ne communique plus avec son extérieur meurt.

Nous préconisons un numérique qui gère de façon différenciée ce qui se passe à l'extérieur, ce qui se passe à l'intérieur et les échanges entre l'intérieur et l'extérieur. C'est ce qu'ont fait les Chinois. Nous ne sommes pas obligés de répliquer le modèle chinois parce qu'il présente des difficultés, mais c'est dans cet esprit que nous devons nous trouver.

Je peux vous dire que, quand nous créons un événement, nous sommes stupéfaits de l'enthousiasme que nous suscitons. Vous vous souvenez sans doute des grands débats en 2018, menés par M. Macron. Nous avons pris l'initiative, avec un consortium de *think tank*s liés au numérique, d'organiser un grand débat avec les quatre thèmes de l'époque, en les traitant uniquement sous l'angle numérique. Nous avons fait salle comble bien que, le même jour, se déroulait un match de foot important, et nous avons dû organiser une deuxième édition.

Je peux vous dire que, quand Cédric O déclare que les Français sont schizophrènes, car ils ont peur des GAFA mais qu'ils n'arrêtent pas de les utiliser, il se trompe. Les Français disent : « Donnez-nous quelque chose d'alternatif. » On nous répond, dans le cadre du débat sur la base de données de santé : « Oui, mais nous sommes obligés d'utiliser la matière américaine parce que la nôtre est trop faible. » En matière de création de richesse immatérielle, il faut comprendre que l'on s'enrichit en utilisant ce que l'on fabrique. Qwant nous l'a très bien montré. Qwant était dénigré pour de multiples raisons, et notamment parce qu'il utilisait le moteur Bing de Microsoft. C'est tout à fait faux, car l'interface joue un rôle extrêmement important puisqu'elle vous anonymise. Du jour où l'on a aidé Qwant à prendre de l'ampleur, Qwant a réalisé des progrès absolument considérables et aujourd'hui, de plus en plus de Français – j'espère que vous en faites partie – utilisent Qwant sans même s'en rendre compte.

Pour revenir aux questions que vous nous posez, il faut prendre conscience de l'histoire réelle du numérique. Les Américains nous ont laissé développer un certain nombre de travaux et, à un moment donné, ils nous ont tordu le bras pour que nous signions des accords pour que nous arrêtions tous nos travaux et que nous leur cédions le passage. Cependant, tous nos travaux n'ont pas quitté le territoire : il s'agit de la richesse immatérielle. Cette richesse immatérielle existe à travers des aînés qui la portent encore et à travers des jeunes qui s'y intéressent de plus en plus. L'élan qu'avait créé French-Road dans la communauté *open source* était tout à fait extraordinaire. French-Road est une communauté de développeurs open source qui ont actualisé les modules de French-Road pour les rendre encore plus « scalables » et actualisés.

Il faut se prémunir contre les dégâts croissants que créent les GAFA et les BATX. Nous allons le faire surtout avec de l'information et de la formation.

Il se trouve que j'ai été dès le départ dans l'association 100 000 entrepreneurs, une association qui demande à des gens qui ont créé des start-up de venir témoigner dans les établissements scolaires et universitaires de façon à ce que les jeunes puissent se positionner par rapport à l'entrepreneuriat. Cette association a le même âge que Forum Atena, une douzaine d'années. Elle connaît un succès extraordinaire. Elle est reconnue par l'éducation nationale.

Quand Cédric O nous parle de formation, je suis très réservée parce que le cursus qui est proposé vise à faire des enfants qui vont devenir des hommes numériques. Je pense qu'il faut en faire des enfants qui vont devenir des avertis du numérique. En parallèle, il faut allumer la petite étincelle qui permet de tirer parti de tout ce patrimoine qui est chez nous, toute la bibliothèque Framasoft, tout ce qu'a fait French-Road… Lancelot va vous parler de tout cela sous un autre angle. Il faut absolument préparer l'après, le numérique 1.0.

Je précise que toutes les solutions concernant les couches basses que nous préconisons à Forum Atena, qui sont essentiellement les couches réseaux (RINA) et les couches immédiatement au-dessus (l'architecture de la donnée, que nous appelons French-Road), ne sont pas incompatibles avec le réseau internet, elles fonctionnent dans la tuyauterie du réseau internet, mais avec une approche, une philosophie qui est radicalement différente.

Dernier point, depuis 20 000 ans, les hommes ont développé la monnaie. La monnaie fonctionne sur la confiance. Quand une monnaie inspire confiance, on l'utilise pour faire du commerce. Le commerce est ce qui a permis de réaliser des progrès techniques et même des progrès sociaux. Là, l'étape sociétale que nous sommes en train de vivre fait que nous allons continuer à faire des progrès techniques, mais c'est surtout des progrès sociaux que nous allons faire, des progrès culturels et des progrès peut-être spirituels aussi. Nous avons besoin de protéger l'environnement. Tout ceci va être fait avec du numérique, de l'échange de données et il nous faut des infrastructures dans lesquelles on échange de la donnée en toute confiance et dans lesquelles les utilisateurs sont engagés parce qu'ils utilisent cette infrastructure.

L'un des problèmes fondamentaux du numérique américain est l'absence d'identification de l'individu, ce qui trouve son explication dans la pensée californienne. Nous, au contraire, à l'époque, nous avions considéré que l'individu était engagé. Nous avions beaucoup utilisé le droit de la presse sur l'engagement. Nous avions bien prévenu les individus qu'ils n'étaient pas des journalistes dans leur prise de parole, mais qu'ils étaient engagés. Un journaliste a une carte de journaliste et, s'il dit des bêtises, il perd sa carte et il ne peut plus exercer. Il s'agit d'une profession réglementée. À propos des professions réglementées, il me semble absolument impératif qu'il existe un ordre des informaticiens : c'est une idée que les Américains ont toujours refusée. *Code is law now*. Le code fait la loi. Il faut que le code soit écrit par des gens assermentés, qui peuvent perdre leur droit d'exercer.

Dernier point, il nous faut des héros. Si vous demandez à un enfant de citer le nom d'un informaticien, il ne citera que des noms américains, qui ont réussi parce qu'ils avaient une équipe autour d'eux. Notre système d'éducation ne sait pas repérer les gens qui ont le profil pour être de grands informaticiens. Il n'existe pas de grande école informatique reconnue dans le système des grandes écoles. Effectivement, jusqu'à maintenant, les grandes écoles sont des écoles inféodées aux éditeurs de logiciels et aux constructeurs d'ordinateurs, et donc à des instances qui ne sont pas les nôtres. Il va falloir inventer quelque chose de nouveau. La tentative avec l'École 42 n'a pas tenu toutes ses promesses. Il nous faut des héros

qui inspirent les jeunes. C'est pourquoi je vous renvoie à ma suggestion autour des 100 000 entrepreneurs.

M. Wilfried Batsch, ancien président d'Opération Lancelot. En mars 2018, nous organisons un débat autour de la souveraineté numérique et, pour une fois, on va entendre la voix des petites et moyennes entreprises (PME) et même des très petites entreprises (TPE), alors que, d'habitude, on n'entend que les grands groupes comme France Télécom-Orange et l'État. L'idée qui a été portée par Julien Irondelle et Éric Lemaire était de dire : « *Pour une fois, on va aller parler à des acteurs plus petits, soit des start-up, soit des PME qui ont déjà une certaine taille comme OVH, mais aussi le petit vendeur sur internet, la TPE de 3 personnes qui vend de la lingerie fine sur internet.* »

Avec toute la matière recueillie, nous avons eu l'idée de lancer une association à destination plutôt des petites entreprises françaises acteurs du numérique. En avril 2019, nous avons réuni Cédric Villani, qui venait de sortir un rapport sur l'intelligence artificielle, et dix acteurs économiques du numérique. Nous avons voulu montrer que tous les secteurs d'activité étaient concernés, y compris des secteurs qui peuvent paraître traditionnels comme l'agriculture. Aujourd'hui, en agriculture, vous avez des drones et de l'intelligence artificielle, vous êtes au cœur de l'activité numérique, les pieds dans les champs. Sur les dix start-up, nous arrivons à faire venir cinq femmes dirigeantes de start-up. Contrairement à ce que l'on croit, le numérique n'est pas une affaire d'hommes.

Nous sommes contents du lancement de cette association que nous appelons Opération Lancelot et nous enchaînons en lançant dans le débat politique, à la faveur des élections européennes. Nous arrivons à faire venir six partis politiques, de l'extrême gauche à l'extrême droite (hormis les Républicains), pour discuter du sujet de la souveraineté numérique. À cette occasion, nous décidons d'inventer un outil de communication, de sensibilisation aux enjeux du numérique, que nous appelons le pacte de la souveraineté numérique. Ce pacte sera un outil formidable pour pouvoir échanger avec les élus. Il va s'enrichir de la confrontation entre les visions politiques et les visions entrepreneuriales des petits acteurs économiques du numérique. En rencontrant les élus, nous allons nous apercevoir que les intervenants sont nombreux dans ce domaine et que nous devons nous démarquer, nous, Opération Lancelot : qu'apportons-nous dans le débat numérique ?

La souveraineté numérique française n'a pas de sens pour nous. Que voulez-vous faire avec 67 millions de clients potentiels quand, en face, vous avez des entreprises qui en ont des milliards ? On ne se pose même pas la question de la souveraineté numérique française même si, au départ, on n'a des acteurs du numérique français. Pour nous, il faut partir sur l'Europe. Vous avez toujours deux façons d'aborder l'Europe : la façon fédérale et la façon internationale symbolisée par le couple franco-allemand. Nous choisissons la deuxième voie : Berlin. Je vais avoir des entretiens avec vos homologues allemands au Bundestag. Je vais m'apercevoir que la souveraineté qui est utilisée dans le langage politique allemand n'a pas tout à fait la même définition qu'en France. Les mots que nous utilisons sont attachés à une culture : or nous n'avons pas la même culture.

Je souhaite en second point, plutôt que répondre tout de suite aux questions que vous nous avez envoyées, parler de cette définition de la souveraineté. Quand vous prenez les constitutions française et allemande, la Constitution de la France commence par définir la République française alors que la Constitution allemande commence par lister tous les droits humains dont bénéficient les citoyens allemands. Cela signifie que, culturellement, la souveraineté pour un Allemand est d'abord personnelle : c'est la souveraineté du citoyen sur ses données, sur son image sur internet, sur sa vie numérique. Alors que la France a été construite par l'État, pas le peuple français. D'ailleurs, vous avez parlé vous-même,

M. Latombe, de « cœur régalien » dans votre introduction. Quand on parle de souveraineté numérique en France, on pense tout de suite à l'État. Ensuite, on dit : « Il n'y a pas que l'État, il faut aussi parler des entreprises », et si possible des grandes entreprises qui ont des liens avec l'État, par exemple Orange, avant de s'intéresser à la TPE au bout de la rue.

La souveraineté politique en France : l'État doit réglementer ce qui se passe sur son territoire. C'est moi le roi de France ou le Président de la République, si je confine, c'est moi qui décide de confiner. Le problème, c'est qu'avec le numérique, on n'est pas sur un territoire physique, on est sur un territoire cyber. C'est ce qui nous a mis complètement à côté. On ne l'a pas anticipé, ni les politiques, ni la société en général. On a des acteurs qui sont basés en Californie : on ne peut pas les fermer. Google a trois grands *data centers* en Europe, en Irlande, en Norvège et en Belgique. Si l'on est capable de tirer sur des terroristes djihadistes au Mali, on est parfaitement capable de détruire ces trois *data centers*. Ce n'est pas le problème. Le problème, c'est que, si vous détruisez ces *data centers*, vous aurez tous les Français qui s'insurgeront parce qu'ils auront perdu leurs courriels et leur photographies hébergés respectivement dans Google Mail et dans Google Drive. Physiquement, l'État français est toujours là avec son armée et ses tribunaux, mais l'acteur est insaisissable : les Français utilisent des services qui sont réglés par des tribunaux américains et qui sont émis par une société dont le siège est basé en Californie.

Comme l'a dit Mme Bouché, il y a des problèmes culturels entre nous et les Américains. Nous sommes des Occidentaux et nous sommes des démocraties. Nous avons donc deux points communs, mais un Californien n'est pas un Parisien. Cela pose un problème de souveraineté culturelle. Qu'est-ce qui choque Facebook basé en Californie ? La nudité. Nous, en Europe, nous sommes choqués, non pas par la nudité, mais par la désinformation. C'est culturel. Avant de décider, au niveau de l'État français ou de l'Union européenne, de réglementer les plateformes, il faut prendre conscience du fait qu'aux États-Unis, ils ne voient pas le même problème que nous.

La souveraineté économique ne repose pas uniquement sur des entreprises. Il ne suffit pas d'avoir un Google français, un Qwant, un OVH, *etc.* C'est là que l'on voit que toutes les souverainetés sont liées. La souveraineté économique, c'est aussi : est-ce que moi, Français, j'ai une chance de trouver un travail ? C'est ma souveraineté économique personnelle, mais c'est un énorme problème pour l'État français si, un jour, nous avons dix millions de chômeurs parce que l'intelligence artificielle a remplacé tous les travailleurs. Je rappelle que notre actuel Président de la République a été auparavant ministre à Bercy et a provoqué un tollé à l'Assemblée nationale en disant : « Un abattoir a fermé quelque part en Bretagne. Le problème, c'est que les salariées femmes sont analphabètes. » Le problème, c'est qu'il avait raison.

Aujourd'hui, nous avons un problème d'« illectronisme » : ce sont des personnes qui savent lire et écrire, mais qui ne savent pas utiliser un portable. Certains ne savent pas déclarer leurs impôts sur internet. Là, on est à la fois dans la souveraineté personnelle et dans la souveraineté politique de l'État qui dit : « J'aimerais bien rationaliser mes administrations, rendre la France plus efficace », comme a dit Mme Bouché. Sauf qu'il faut former les gens. S'il n'y a plus de guichet pour déclarer ses impôts et que tout passe par internet, il faut que tout le monde sache le faire. Et l'on a un problème économique : il faut que tout le monde sur le territoire puisse au moins accéder à la 4G, ce qui n'est pas tout à fait le cas aujourd'hui.

L'on voit bien qu'il existe plusieurs niveaux de souveraineté qui sont tous imbriqués et qui s'influencent mutuellement. Je pense qu'il faut l'avoir présent à l'esprit. Le numérique est vraiment une nouvelle civilisation, qui couvre tous les aspects. Je trouve intéressant que Mme Bouché ait mentionné la spiritualité. Il est vrai que la spiritualité, avec internet, cela peut

changer. Je ne sais pas si l'on peut appeler cela de la spiritualité, mais pourquoi des Français sont partis faire le djihad en Syrie ? Parce qu'ils ont vu des vidéos sur Facebook. Nous avons un problème de souveraineté là aussi. Nous avons des gens qui n'écoutent plus ce qu'écoute le prof à l'école. Ils préfèrent aller regarder sur Facebook ce qui se passe en Syrie pour aller faire la guerre là-bas ! Ou maintenant en Arménie.

Beaucoup de choses s'imbriquent entre elles. C'est pour cela que c'est passionnant que vous soyez issus de plusieurs commissions. Effectivement, cela touche toutes les commissions, mais à mon avis notamment la commission éducation et culture parce que l'un des gros enjeux est l'intelligence artificielle. Les avocats sont titulaires d'un bac + 5. Maintenant, vous avez des *legal tech* qui peuvent vous faire des procédures automatisées par algorithme. Comment l'avocat va-t-il gagner sa vie si, au lieu de payer 2 000 euros, vous trouvez à peu près la même prestation sur internet pour 200 euros ?

Dans toutes les auditions que nous avons menées avec Opération Lancelot d'acteurs économiques et d'acteurs politiques, pour moi, cette question est centrale : c'est la souveraineté personnelle. Ce n'est pas juste ce que fait Google ou Facebook de mes données, c'est : est-ce que moi, dans vingt ans, j'ai encore un travail ? La souveraineté de l'État français, c'est de ne laisser personne sur le bord de la route. Sinon, la France n'existe plus. Si dix millions de personnes sont en dehors du système, avec juste le RSA (revenu de solidarité active) parce qu'elles ne savent pas vivre dans une civilisation numérique, à terme, on est mort.

Voilà pour mon introduction. Voulez-vous que je réponde maintenant aux questions que vous nous avez envoyées ?

M. Philippe Latombe, rapporteur. Oui, allez-y.

Mme Geneviève Bouché, présidente du Forum Atena. Je voudrais revenir sur le problème de la fiscalité. Aux États-Unis, les GAFA sont même pointés pour leur comportement vis-à-vis de la fiscalité puisqu'ils essayent de mettre leurs profits dans des paradis fiscaux. Un de leurs arguments est le suivant : « Les usagers me donnent la matière première, il n'y a donc pas de transfert de propriété, je les transforme en Californie ou ailleurs, en tout cas, je ne les transforme pas là où ensuite, la valeur va être réellement créée. » Effectivement, où prélève-t-on les taxes ? Là où la valeur est utilisée ou là où la valeur est créée ? Les GAFA défendent l'idée qu'il faut taxer là où la valeur est créée et c'est pour cela qu'ils ne payent pas d'impôt chez nous.

Le numérique étant une économie de l'immatériel par excellence, il faut absolument faire évoluer les taxes pour taxer là où la valeur est mise en valeur en quelque sorte. Les données que collecte Facebook servent à faire des profils et, ce qui est beaucoup plus grave, à faire des bulles d'influence. Ces profils servent à servir la bonne publicité à la bonne personne au bon moment. C'est là où l'on sert la publicité qu'il faut prélever la taxe. Je me permets d'insister là-dessus parce que c'est un point absolument fondamental. Je suis très étonnée quand j'entends les débats. C'est assez bizarre, les gens ne comprennent pas ce que je suis en train de dire. J'espère que vous, vous me comprenez.

M. Wilfried Batsch, ancien président d'Opération Lancelot. Je vais laisser Éric Lemaire répondre à vos questions.

M. Éric Lemaire, président d'Opération Lancelot. Je suis entrepreneur. Je dirige un groupe d'une centaine de personnes dans l'informatique avec une dizaine de filiales et une vingtaine d'investissements. Comme vous l'a dit Wilfried, il y a deux ans, nous avons organisé une conférence. J'y ai participé parce que l'une de mes filiales est un site de commerce en

ligne et un quart de son chiffre d'affaires est consacré à la publicité sur un GAFA dont le nom commence par G. D'une part, ce GAFA, aussi bien intentionné soit-il, a des changements de politique commerciale, de politique tarifaire, d'organisation et fait donc peser sur la survie même de l'entreprise en question une menace insupportable. D'autre part, il nous envoie tous les mois des factures de 50 000 à 100 000 euros, sans TVA, en provenance d'un paradis fiscal bien connu. Non seulement nous sommes totalement dépendants, mais en plus, une bonne partie de leur avantage compétitif sur les gens qui font partie d'Opération Lancelot est constitué par cet avantage fiscal.

Nous nous sommes lancés dans Opération Lancelot pour essayer de convaincre un certain nombre d'acteurs du monde de l'entreprise. Comme cela a été dit tout à l'heure, il n'y a pas que le politique, nous autres, les entrepreneurs, nous sommes aussi responsables de ce qui est en train de se passer et nous devons nous y investir. Nous devons faire l'effort d'utiliser des locaux et de nous mettre ensemble. L'État a fait beaucoup pour nous. J'ai l'âge où, quand on créait une entreprise, il fallait s'affilier aux trente caisses de retraite. Cela a été supprimé. Vous avez créé la BPI, vous avez créé les jeunes entreprises innovantes, vous avez créé le crédit d'impôt recherche (CIR). Beaucoup de choses ont changé, ce qui fait qu'aujourd'hui, il existe un terreau de PME. Pourquoi ne grandissent-elles pas ?

Nous avons parmi nos membres un dirigeant, Philippe Kalousdian, qui a une société de conseil dont le métier est de digitaliser des entreprises. Il a interviewé un certain nombre de grands comptes et de fondateurs de grosses start-up et leur a demandé pourquoi nous n'avions pas de GAFA. Il a eu un certain nombre de réponses classiques : le manque de culture de langue étrangère, les écarts culturels… Une réponse nous a beaucoup surpris : l'Europe n'est pas un marché unique. Quand Criteo par exemple a voulu s'installer dans 27 pays, il s'est retrouvé face à 27 droits, 27 droits du travail, 27 droits fiscaux, 27 droits des sociétés, cela lui a coûté une fortune, 20 à 30 % de leur levée de fonds. Pour acquérir une *market dominance*, il a dû dépenser un quart d'argent en plus que ce qu'aurait fait leur équivalent américain en Amérique. C'est une grosse difficulté. Il faut que l'Europe acquière son indépendance.

Trois univers, les États-Unis, la Russie et la Chine, ont chacun leurs GAFA. L'on ne peut pas dire que la Russie est plus puissante que nous économiquement.

Le deuxième sujet qui mérite d'être mentionné ici, c'est l'aspect marchés publics. Dans ces trois autres ensembles, cela n'existe pas d'avoir plus de 10 % de marchés attribués hors secteur. En Europe, ce n'est pas le cas. Il faut qu'il y ait de la réciprocité.

Troisième point, c'est ce que nous, les entrepreneurs, appelons « la vallée de la mort ». Il est relativement facile de faire une levée de fonds de 100 000 euros. Il est possible de faire une levée de fonds de 10 millions d'euros. Il est facile de se vendre pour 50 millions d'euros. En revanche, lever 2 ou 3 millions d'euros est extrêmement difficile. L'un de nos membres, Whaller, le réseau social éthique pour entreprises, est dans cette démarche. Il s'agit d'une magnifique entreprise, qui est en croissance et qui est rentable. Ils ont de réelles difficultés à faire ce type d'opération. Il faut que l'on redirige l'épargne des Français vers les PME de croissance.

Vous avez fait aussi un merveilleux travail culturel à l'échelon national. Désormais, l'entrepreneur n'est plus mal vu. Il est très facile pour nous de recruter des gens dans nos structures. Par contre, nous n'avons pas de culture d'investissement dans les PME. Plan d'épargne entreprise, cotisations retraite ou que sais-je, il faut essayer de trouver une solution.

Que va-t-il nous arriver si l'on continue comme cela ? Ce qui nous arrive maintenant, c'est que 3 milliards d'euros par mois sortent de notre région et partent dans un paradis fiscal

qui, parfois, se trouve en Europe, sans donner de nom, puis sont transférés ailleurs. Si l'on continue comme cela, il va nous arriver la même chose dans le secteur des transports, dans le secteur de la santé, dans le secteur de la culture et au lieu de voir 3 milliards d'euros partir tous les mois, ce sera 15, 20, 25. J'ai des amis entrepreneurs libanais qui, aujourd'hui, quand ils doivent acheter de la matière hors Liban, sont obligés d'aller chercher des dollars au marché noir : c'est un cauchemar parce qu'ils ont perdu leur indépendance, ils n'ont pas une balance commerciale équilibrée et ils ont besoin d'être aidés. Nous devons trouver une solution avant. La Russie a réussi à la trouver avec relativement peu de contraintes. Ce n'est pas tout à fait notre culture, mais ils ont réussi à le faire alors qu'ils n'avaient pas la puissance économique des Américains ou des Chinois. En plus, ils sont partis plus tard.

Sur les domaines spécifiques que l'on serait en mesure d'investir, tout d'abord, je voudrais dire que nous n'avons perdu. Aujourd'hui, dans Lancelot, la société E-corp développe un système d'exploitation pour téléphone et vend dans toute l'Europe, en particulier en Allemagne. Nous avons une autre start-up qui s'appelle Hyperpanel qui développe un système d'exploitation personnel. Les systèmes d'exploitation, c'est là où transite la donnée, c'est cela que l'on veut protéger. Nous n'avons pas perdu, pas du tout.

Je souhaitais vous parler de deux domaines : l'informatique imprimée et l'informatique verte.

Nous avons de magnifiques start-up et même des entreprises en Europe qui font de l'informatique imprimée. Cela nous permettrait d'échapper à l'influence de l'Asie du Sud-Est. Si nous imprimions nos propres puces avec des imprimantes 3D, nous n'aurions plus de problèmes de fondeurs, nous n'aurions plus de problèmes de dépendance à l'Asie.

Nous avons en Europe les meilleurs systèmes de refroidissement par liquide. C'est un double gain de souveraineté. Non seulement on achète du matériel en Europe plutôt qu'à l'extérieur, mais en plus, on consomme beaucoup moins. Aujourd'hui, on a la possibilité de diviser par dix rapidement l'empreinte écologique de l'informatique bureautique, ce qui aurait un impact phénoménal sur notre consommation d'électricité et de matière.

Le dernier point que vous avez soulevé concernait la sécurité. En tant qu'entreprise du numérique, nous avons de nombreux clients qui ont beaucoup d'ennuis avec des *ransomewares* (logiciels malveillants). Nous avons de grosses entreprises qui se sont retrouvées en procédure de sauvegarde parce qu'elles ont subi des attaques informatiques. Il faut faire le même travail sur la protection des systèmes que celui qui a été fait au niveau européen sur la protection des données avec le RGPD (règlement général sur la protection des données). Il faut en finir avec la naïveté y compris dans le secteur privé. Il n'y a pas de raison que nous perdions toutes nos données sous prétexte que nous n'avons pas un *firewall* (pare-feu) ou que nous avons des mots de passe peu sécurisés.

Nous autres, entreprises du numérique, nous ne pouvons pas donner d'argent à un parti politique en France, et c'est tant mieux. Pourquoi sur internet peut-on financer des idées politiques sans aucun contrôle ? Je ne comprends pas. Je pense qu'il faut faire dans le monde numérique le travail qui a été fait dans le monde physique. Il faut un minimum d'éthique et mettre les lois qui nous correspondent.

Je suis à votre disposition pour répondre à vos questions.

M. Philippe Latombe, rapporteur. Mon collègue Pierre-Alain Raphan ne pouvait pas être là aujourd'hui, mais il m'a transmis une question. Vous l'avez effleurée en parlant des marchés publics. Avez-vous, les uns et les autres, identifié d'autres actions ou processus que

nous faisons et qui nous sabordent dans cette recherche de la souveraineté ? Avant de chercher à créer quelque chose d'autre, n'y a-t-il pas des actions négatives que l'on devrait arrêter rapidement ? Sur les marchés publics, vous avez demandé que l'on arrête d'avoir cette absence d'exigence de réciprocité. Avez-vous identifié d'autres sujets ?

M. Wilfried Batsch, ancien président d'Opération Lancelot. Dans le cadre de notre pacte de la souveraineté numérique, nous avions pensé à un *small business act* qui ne peut pas être français compte tenu des lois sur la concurrence dans l'Union européenne. En revanche, l'on peut passer par un autre biais, privilégier le local. C'est peut-être envisageable dans le cadre de la réglementation communautaire. Quand vous faites une activité partielle, vous allez privilégier votre tissu local. Il me semble que, dans les autres pays européens, c'est une idée qui pourrait être acceptable, y compris dans les pays plus libéraux que la France. Le discours que tiennent beaucoup d'entrepreneurs d'Opération Lancelot ou d'ailleurs est de dire : « Nous ne quémandons pas des subventions, nous voulons des contrats, mais nous n'avons aucune chance. » C'est un problème culturel.

Vous nous avez demandé : « Estimez-vous que la France dispose des bons outils pour défendre une souveraineté industrielle ? » Nous n'avons pas les bons outils culturels parce qu'en France, l'administration veut tout faire elle-même. Aux États-Unis, ce n'est pas l'administration qui a créé Amazon. Par contre, l'administration a dit : « Je vous donne tant de milliards si vous me faites ce que je veux. » En France, l'administration dispose de ressources humaines très compétentes et chaque ministère, voire chaque direction au sein d'un ministère, a ses propres solutions. Il y a là une réflexion à avoir qui, avant d'être une réflexion juridique, est une réflexion culturelle. Pourquoi les Américains sont-ils bons ? Parce que l'administration ne veut pas faire elle-même, mais signe des contrats avec des entrepreneurs pour qu'ils fassent à sa place.

Mme Geneviève Bouché, présidente du Forum Atena. Ce qui a fait la force de la France, c'est son esprit cartésien et son fonctionnement en silo. Cela nous a permis jusqu'à maintenant d'être très efficaces. Le monde qui vient est un monde en rhizome, en réseau et l'architecture système dont je vous ai parlé et qui convient à l'Europe – c'est le cœur du système estonien – est complètement en réseau. L'information doit être partagée, dès lors que l'utilisateur a été agréé pour utiliser cette information. Il faut faire une bascule culturelle en France pour sortir de l'esprit silo.

Forum Atena a fait un chantier assez important sur la notion d'État plateforme, au sens d'infrastructures de la donnée publique. On ne peut pas aller vers une notion d'État plateforme tant que l'on a une administration qui continue à s'informatiser comme on le faisait dans les années 60. Dans les années 60, on prenait un service et on transposait en informatique ce qui existait. Aujourd'hui, il faut avoir une vision globale du schéma d'information et faire en sorte qu'une administration nourrisse et se nourrisse du schéma global. C'est avec ce type d'architecture que l'on va pouvoir sortir de cette organisation en silo qui nous pèse énormément et qui fait que l'on a des systèmes lourds, peu fiables et surtout excessivement coûteux à entretenir. Quand vous rentrez dans le siège social de X-Road en Estonie, vous tombez sur une Tour Eiffel, pour symboliser le fait qu'avec leurs 1,4 million de ressortissants, ils économisent grâce au système la hauteur d'une Tour Eiffel de papier par mois. Cette notion de silo qui a été notre force est devenue notre faiblesse aujourd'hui et le numérique peut jouer un rôle excessivement important.

Je reviens sur les problèmes de financement. Il se trouve que je suis la cofondatrice de Dauphine Business Angels. Dauphine étant la faculté des traders, nous avions beaucoup à dire et à faire dans ce domaine. La traversée du désert est un scandale. Il faut prendre ce problème à bras-le-corps. J'ai eu l'occasion d'échanger avec Bruno Le Maire sur ce sujet et je lui ai que

je n'arriverai pas du tout à comprendre que nos start-upers quand ils voulaient s'installer à l'étranger n'arrivaient pas à lever des fonds à l'étranger alors qu'il s'agit de la bonne stratégie. Quand on veut aller en Belgique, on n'arrive pas à lever des fonds belges pour s'installer en Belgique. Il faut développer toute une culture. L'Europe, dans son design actuel, a été conçue pour faire en sorte que les pays européens ne se fassent pas la guerre. Là, il faut franchir une étape : il faut que les pays européens construisent l'Europe et ils vont la construire avec un tissu entrepreneurial. La BPI est française. Dans les mécanismes de levée de fonds, il faut susciter un partenariat trans-nations.

Les questions que vous soulevez sont immenses. Chacune mériterait une matinée. Nous essayons de distiller les points les plus saillants.

M. Éric Lemaire, président d'Opération Lancelot. Depuis l'affaire Cambridge Analytica, je ne comprends pas pourquoi l'on utilise encore Facebook dans les milieux publics. Sachez qu'en Russie, quand vous êtes dans la fonction publique, vous recevez un livret de consignes et, parmi ces consignes, figure celle de coller un scotch sur la caméra de votre ordinateur pour ne pas être surveillé. Je pense qu'il faut perdre notre naïveté aussi bien dans le public que dans le privé.

M. Philippe Latombe, rapporteur. Dans Opération Lancelot ou Forum Atena, vous avez des entrepreneurs qui ont eu parfois des succès et parfois des échecs. Avons-nous des changements à opérer, techniquement et administrativement, dans l'acceptation culturelle de l'échec ?

Mme Geneviève Bouché, présidente du Forum Atena. Je pense que l'on peut déjà prendre le problème à la racine. Vous savez que tout ce qui concerne le droit est très chahuté par le numérique. Entre autres choses, nous avons un traitement pathétique des tribunaux de commerce. Nos start-up numériques sont traitées comme toutes les autres sociétés dans les tribunaux de commerce avec des mandataires liquidateurs qui jettent le brevet par-dessus bord. L'on dit souvent que les tribunaux de commerce sont un hôpital dont on sort mort systématiquement. Il faut réformer d'urgence les tribunaux de commerce pour que ce soit des lieux de recyclage. J'ai travaillé avec l'École centrale sur un concept de « débutance ». L'équipe qui a fabriqué Criteo est extrêmement brillante, mais avant d'avoir un Criteo, il y a eu une douzaine de start-up qui ont essayé, mais qui n'ont pas été comprises par l'environnement. De même qu'aujourd'hui, recycler les déchets commence à devenir une évidence, il faut recycler nos start-up. Pourquoi ne pas expérimenter une nouvelle juridiction commerciale dans le numérique puisqu'il faut absolument recycler l'immatériel qu'il contient, c'est-à-dire les talents et les savoirs, à travers l'expérience ?

M. Éric Lemaire, président d'Opération Lancelot. Je vais prendre un exemple. Il n'y a pas longtemps, j'ai vu un rachat se faire à la barre du tribunal d'une société qui était assez mal en point. Cette société détenait un fichier. Compte tenu du nouveau RGPD, dans ce fichier, il n'y avait pas toutes les informations que l'on pouvait avoir. Cet exemple illustre ce qui vient d'être dit sur la nécessité d'une juridiction. Les conditions de revente d'actifs numériques, les conditions sur les plus-values, l'acceptation de l'échec dans la façon dont les lois sont écrites… *Code is law*. De la façon dont le code est écrit découle le changement à long terme de la culture. En France, on a acquis une culture de l'entrepreneuriat et de la start-up ces quinze dernières années. Aujourd'hui, nous avons peut-être plus de petits entrepreneurs qu'aux États-Unis. Il faut simplement continuer cette mutation en l'écrivant dans nos codes juridiques, et cela infusera tout seul, je pense.

Mme Geneviève Bouché, présidente du Forum Atena. J'ai vécu la fabrication de la Silicon Valley. La Silicon Valley est un plan général. Je les ai vus dérouler leur plan avec

détermination et énormément de souplesse. En Asie, il y a des ministres de l'innovation. L'innovation se manage. En France, nous n'en avons pas. Vous nous posez de façon insistante la question : que faut-il faire ? Il faut faire une stratégie à long terme. Qu'est-ce que nous ne voulons pas ? Qu'est-ce que nous voulons ? Qu'est-ce qu'il nous manque pour le faire ? Sur quoi pouvons-nous nous appuyer ? Comment pourrons-nous le faire ? Je précise qu'il s'agissait du cœur de ma formation à Dauphine et que cette formation a été fermée en 1977. Je pense qu'il faudrait la recréer.

M. Éric Lemaire, président d'Opération Lancelot. Je voudrais ajouter un point : dans l'innovation, il y a aussi les collaborations public-privé. J'ai eu l'occasion de le faire avec des universités sur le plateau de Saclay. Le transfert de brevets partiellement publics vers le privé ou les collaborations de recherche sont loin de marcher comme elles le devraient. Dans la structure de notre produit intérieur brut (PIB), il n'y a pas suffisamment d'argent qui est consacré à l'innovation entre le public et le privé parce que le rouage entre les deux ne fonctionne pas bien. Il faut absolument réformer le système de transfert. Par exemple, en tant qu'entrepreneur, j'aimerais que l'on me dise « Si vous voulez utiliser un brevet d'État ou travailler avec un laboratoire d'État et que de la propriété industrielle est créée, voilà le contrat type, voilà les pourcentages » avant, et pas après. C'est source de contentieux sans fin et source d'absence de recherche de certains acteurs économiques qui innovent tout le temps et qui savent que, s'ils travaillent avec un laboratoire public, cela ne va pas bien se passer.

Mme Geneviève Bouché, présidente du Forum Atena. Le point que vous soulevez, je le connais bien. Il s'agit de blocages idéologiques, qui datent des Trente Glorieuses. Les textes sont en bon état : il faut simplement les faire appliquer.

M. Philippe Latombe, rapporteur. Partagez-vous ce point de vue ou pensez-vous qu'il faut quand même réformer les contrats ?

M. Éric Lemaire, président d'Opération Lancelot. Effectivement, des efforts ont été réalisés, mais mon point critique est que, dans les collaborations entre public et privé, la rémunération est définie à la fin et pas au début. Or, en tant qu'entreprise privée, je veux savoir au début combien cela va me coûter. Le problème est en grande partie culturel.

M. Philippe Latombe, rapporteur. Merci beaucoup. Nous arrivons à la fin du temps qui nous était imparti. Y a-t-il des points que vous souhaiteriez encore aborder ?

Mme Geneviève Bouché, présidente du Forum Atena. J'aimerais que vous nous parliez de votre mission. Combien de personnes allez-vous auditionner ? Comment les avez-vous choisies ? Comment allez-vous traiter les travaux ? Aurons-nous un retour ?

M. Philippe Latombe, rapporteur. La mission dure un an. Nous regardons quels sont les différents aspects dans la souveraineté pour voir ensuite comment concrètement nous pouvons mettre en œuvre des solutions qui permettent, non pas de révolutionner les choses, mais de commencer à amorcer la construction d'une souveraineté française et européenne. Dans le titre de la mission, nous avons mentionné « française et européenne », car un certain nombre de leviers ne peuvent être actionnés qu'au niveau européen. L'idée est de pouvoir rendre un rapport avec des propositions concrètes en juin 2021. La mission est composée de représentants de toutes les sensibilités politiques et de différentes commissions. Nous sommes dans une phase d'auditions relativement larges autour des problématiques communes : la partie matériel, l'intelligence artificielle, la partie des logiciels, la *blockchain*… Nous sommes humbles et nous allons nous inspirer des rapports qui ont déjà été faits pour les transformer en propositions concrètes.

Mme Geneviève Bouché, présidente du Forum Atena. Ce que vous faites est-il fait aussi dans d'autres pays européens ou est-ce une initiative franco-française pour le moment ?

M. Philippe Latombe, rapporteur. Il s'agit d'une initiative de l'Assemblée française, mais nous avons des contacts avec l'Union et un certain nombre de parlementaires d'autres pays dans lesquels une réflexion est menée. Nous allons essayer de trouver des concordances pour avoir des initiatives si possible communes ou, en tout cas, qui ne soient pas antagonistes. Il faut, comme vous l'avez dit tout à l'heure, éviter que l'on ait 27 droits et 27 initiatives qui soient toutes les unes antagonistes par rapport aux autres.

M. Wilfried Batsch, ancien président d'Opération Lancelot. Il me semble que l'on a toujours ce partenariat franco-allemand en Europe qui est capital. J'ai été très surpris de découvrir l'existence d'une assemblée parlementaire franco-allemande entre l'Assemblée nationale et le Bundestag. Il s'agit d'un saut qualitatif dans les relations franco-allemandes parce qu'avant, les discussions ne se déroulaient qu'entre le Président de la République française et le chancelier fédéral allemand. Cette assemblée a en plus un groupe de travail permanent sur les ruptures technologiques qui a été initié côté français par Christine Hennion et par une députée allemande écologiste. Dans le cadre de vos travaux, vous pourriez vous rapprocher de cette commission franco-allemande, car, comme toujours, quand on travaille entre Français et Allemands, cela élargit tout de suite les possibilités.

Dernier point, des élections partisanes, internes au SPD, se sont déroulées en novembre 2019. Quel est le profil de la nouvelle coprésidente du SPD ? Elle a été ingénieure informatique avant d'être députée.

M. Philippe Latombe, rapporteur. Cela fait partie du périmètre que nous allons aborder. Nous avons au sein de la mission des députés qui font partie du groupe de travail franco-allemand.

Audition, ouverte à la presse, de M. Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique *(29 octobre 2020)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Je suis très heureux de vous accueillir, monsieur Benhamou. Vous êtes secrétaire général de l'Institut pour la souveraineté numérique (ISN). Notre mission d'information va, pendant plusieurs mois, se pencher sur moyens de bâtir et de promouvoir une souveraineté numérique européenne et française. Aussi nous apparaît-il indispensable de recueillir l'analyse de l'Institut que vous représentez parce que son objet de travail est identique à celui de notre mission.

À cet effet, nous souhaiterions que vous nous présentiez en quelques mots votre organisation, sa genèse, son mode de fonctionnement ainsi que ses activités.

Le thème de la souveraineté fait immédiatement appel au cœur régalien des missions de l'État, mais nous engage également à une réflexion sur les armes économiques dont nous devons disposer pour défendre la place de notre pays et de l'Union européenne dans la compétition mondiale. Sur ces deux plans, régalien et économique, nous aimerions connaître votre opinion sur la montée en puissance de la notion de souveraineté numérique. Comment l'analysez-vous ? Que pensez-vous des positions adoptées au niveau national et européen sur ces sujets par les autorités publiques ? Quelle appréciation portez-vous sur les initiatives législatives en cours ?

Cette problématique de souveraineté numérique implique de nombreux sujets souvent porteurs d'enjeux majeurs pour la place de notre pays sur la scène internationale. Nous pensons en premier lieu aux questions de cybersécurité et de cyberdéfense. Ici, la thématique de la souveraineté est incontournable puisqu'il s'agit de déterminer comment protéger les intérêts français de nouvelles menaces immatérielles et déterritorialisées. Il s'agit également de définir de nouvelles modalités de discussions avec nos partenaires européens et autres pour engager des actions concertées, mais respectueuses de la souveraineté de chacun. Quelle est votre analyse de ces enjeux multilatéraux ? Comment percevez-vous le paysage international actuel ? Quelles devraient être, selon vous, les réponses françaises et européennes aux menaces de déstabilisation ou de désinformation ?

La souveraineté numérique française et européenne est aussi, sur un mode peut-être moins visiblement conflictuel, confrontée à la montée en puissance de nouveaux acteurs privés qui prétendent imposer leurs normes ou qui disposent d'un pouvoir de marché les rendant bien souvent incontournables pour les consommateurs et les usagers. Comment la France et l'Union européenne peuvent-elles, selon vous, reprendre la main sur la définition des termes dans ces rapports nouveaux afin de ne pas être réduites à une position strictement réactive, voire passive ? Nous pourrons ici évoquer les multiples instances privées ou semi-privées dans lesquelles s'organise la gouvernance d'internet, l'attribution des noms de domaine par exemple, tout comme les géants du numérique qui jouent un rôle de prescripteur de plus en plus important dans nos sociétés, qu'il s'agisse des modes de consommation ou de notre façon de nous informer. La crise que nous traversons ne fait que renforcer malheureusement ces tendances. Quelle réponse publique apporter, selon vous, au plan national, européen et international ?

Enfin, la défense de la souveraineté numérique passe aussi par celle d'une certaine autonomie matérielle et par la défense et la promotion d'une industrie du numérique européenne compétitive et indépendante. Or nous savons que l'Europe souffre de façon croissante du départ d'industries stratégiques pour le matériel informatique qui constituent pourtant le soubassement du développement du numérique. La dépendance aux solutions technologiques extracommunautaires (aussi bien logiciels que matériels) met-elle en cause, selon vous, l'autonomie européenne ? Comment contrer cette tendance et comment faire participer l'innovation et la recherche à une certaine forme de réindustrialisation dans les nouvelles technologies à même d'assurer une plus grande souveraineté européenne ?

Je vous laisse la parole en espérant que nous pourrons balayer l'ensemble de ces sujets pendant l'heure qui nous est impartie. En tout cas, je vous remercie de vos commencements de réponse.

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. D'abord, l'ISN a maintenant six ans. Nous l'avons conçu en 2014-2015. À l'époque, la première question que l'on nous posait était : « Qu'est-ce que la souveraineté numérique ? » Je suis heureux de voir qu'après quelques années, on ne nous la pose plus. Aujourd'hui, le thème de la souveraineté numérique est devenu plus familier, parce qu'il est abordé quasiment quotidiennement dans la presse, mais tel n'était pas le cas à l'époque, quand nous avons créé l'Institut.

L'ISN est une association loi de 1901, qui rassemble des personnes de tous horizons (universitaires, entrepreneurs) et qui a été fondée sur l'idée que la question de la souveraineté numérique, qui apparaissait à peine dans le champ des experts et des régulateurs à l'époque, allait devenir importante.

À l'évidence, nous ne nous sommes pas trompés. Aujourd'hui, particulièrement du fait de la pandémie, l'on a pu se rendre compte encore plus de notre dépendance technologique à des solutions et à des acteurs extra-européens. En cette reprise de confinement, l'on se rend compte de l'importance, voire du déséquilibre que cela crée par rapport à notre tissu économique traditionnel. Fondamentalement aujourd'hui, l'on se rend compte de la véracité d'un propos que l'on avait tenu il y a quelques années qui consistait à dire qu'à mesure que les États utilisent les technologies, la souveraineté numérique devient indiscernable des outils technologiques. Quand il est question de défense, de sécurité, de sécurité sanitaire, de régulation des villes, d'éducation, de pratiquement tous les sujets sur lesquels la puissance publique a à se prononcer, aujourd'hui, le numérique a une part déterminante.

Je précise que j'ai aidé à créer l'ISN après avoir exercé les fonctions de délégué interministériel aux usages du numérique et, auparavant, de m'être beaucoup occupé au sein de l'État et de différents ministères des questions de régulation de l'internet, en particulier lors du sommet des Nations unies sur la régulation de l'internet en tant que conseiller de la délégation française. Ce sont des sujets qui maintenant sont montés en puissance. Vous parliez des grands acteurs non européens, qu'ils soient américains (Google, Apple, Amazon, Microsoft) ou chinois (Baidu, Alibaba, Tencent, Huawei, Xiaomi). Il manque dans ces acronymes des lettres européennes. S'il est bien une feuille de route pour la France et pour l'Europe dans les temps qui viennent, c'est bien de rajouter des lettres européennes dans ces acronymes.

Or, nous n'avons pas de grands acteurs de taille internationale dans ces domaines, ce qui est un prérequis indispensable si l'on ne veut pas agir que juridiquement. Quelle que soit l'efficacité des actions antitrust, quelle que soit l'efficacité des actions fiscales, quelle que soit l'efficacité des mesures de régulation que l'on peut être amené à prendre, si l'on n'a pas une industrie européenne forte dans ces domaines, ce qu'a rappelé Charles Michel, le président du

Conseil européen, et Thierry Breton, le commissaire européen au marché intérieur, si l'on n'a pas une industrie capable de concurrencer, voire de créer de nouvelles normes, de nouveaux standards dans ces domaines, comme l'a dit Sigmar Gabriel, l'ancien vice-chancelier allemand, tous les débats que nous évoquons aujourd'hui seront sans objet. Pour être un peu spécialiste de ces questions, pour l'enseigner à Panthéon-Sorbonne ou à Sciences Po auparavant, la régulation ne peut pas tenir si nous n'avons pas les acteurs.

Vous parliez de régulation à la fois sur les questions régaliennes et sur les questions économiques. La particularité réside dans le fait qu'il n'est pas de champ de l'activité économique de l'activité des États, des activités humaines de manière générale qui ne puisse de près ou de loin être transformée (« ubérisée ») par les acteurs numériques.

Auparavant, il existait des secteurs industriels qui étaient relativement stables (l'automobile, l'agriculture, le luxe, les transports…). Aujourd'hui, des acteurs qui n'ont aucune expérience préalable, aucune infrastructure préalable sont capables de s'insérer, de modifier, de transformer l'ensemble des modèles économiques. Ainsi, le groupe Accor, le célèbre groupe hôtelier français, n'imaginait pas il y a dix ans être confronté à un concurrent mondial, Airbnb, qui n'a possédé pendant très longtemps en propre aucune chambre d'hôtel, mais qui a été à même de vendre des nuitées partout sur la planète en l'espace de quelques années.

Pour l'instant, nous sommes en situation hautement défensive. Je crois qu'il nous faut absolument réfléchir à une possibilité de rebond, à une nécessité de rebond par rapport à cela. Cette nécessité doit prendre appui sur les faiblesses que nous notons aujourd'hui dans les acteurs du numérique, faiblesses en termes de confiance, faiblesses en termes de sécurité et de protection des données, faiblesses en termes de protection des processus démocratiques. Hier, les principaux patrons des réseaux sociaux étaient auditionnés au Sénat américain. L'on doit se poser la question de savoir dans quelle mesure on n'a pas laissé se produire des phénomènes tant en Europe qu'au niveau international de remise en cause des processus démocratiques. La triste actualité de ce matin nous rappelle les effets néfastes de la radicalisation algorithmique.

Ces plateformes, en plus d'exercer une influence de marché considérable, d'abuser très régulièrement de leur position dominante, de leur position monopolistique ou oligopolistique, ont un modèle économique basé sur la donnée personnelle. En termes techniques, on parle de « micro-profilage », c'est-à-dire de profilage extrême des individus. Ce modèle économique hyper-centré sur la donnée est toxique. Comme le disait une sociologue il y a quelque temps dans le *New York Times*, il n'existe pas de complicité entre le mouvement extrémiste djihadiste, suprématiste, *etc.* et les plateformes comme YouTube, mais il existe une convergence d'intérêts toxique.

Pourquoi ? Parce que l'algorithme de recommandations de YouTube intègre le fait que plus une vidéo est radicale (« hardcore »), plus elle est addictive et plus elle est addictive, plus les gens vont consommer de la publicité en la regardant. La radicalité, le côté clivant, polarisant, est utile à des plateformes comme Facebook ou comme YouTube et peut-être aussi sous une autre forme pour Twitter.

Nous avons laissé se construire ces sociétés en considérant que la donnée était l'or noir, le pétrole du siècle numérique, ce qui est très dangereux parce que cela tend à montrer que l'humain devient une matière première, une variable d'ajustement dans le fonctionnement de la société numérique. Je crois qu'il est important que la souveraineté numérique soit fondée, que l'action numérique européenne et française soit fondée sur les principes et les normes que nous défendons au sein de l'Union. Je citais les équivalents chinois des GAFA américains, Baidu, Alibaba, Tencent, Xiaomi, qui se sont développés en voulant reproduire le modèle économique d'Amazon, de Google, de Facebook et d'Apple.

Nous devons avoir une vision innovante. Charles Michel, dans sa récente conférence de presse sur ces sujets, disait qu'il y avait un espace pour des technologies qui ne seraient pas menées soit par cette dérive liée à l'acquisition de plus en plus importante de données sur les individus, ce qui est le cas des grandes sociétés américaines, soit par cette vision autoritaire telle que la Chine la déploie chaque jour davantage autour du crédit social, c'est-à-dire ce système de notation orwellien des individus, une notation qui leur permet ou pas d'accéder à des droits fondamentaux comme celui de se déplacer en train ou en avion, d'accéder à un crédit ou à une promotion… Dans beaucoup de domaines, il s'agit d'un outil d'ingénierie sociale et de contrôle social extraordinaire efficace. Je précise que l'application de maîtrise de la covid en Chine qui a été élaborée par Alibaba est aussi un outil redoutable dans la mesure où l'on peut interdire de façon discrétionnaire l'accès à tel ou tel bâtiment, tel ou tel lieu public, tel ou tel service par l'intermédiaire d'un code que l'on doit scanner à l'entrée de chaque immeuble.

Quel modèle de civilisation voulons-nous ? C'est la seule bonne question qui vaille. Voulons-nous d'une civilisation qui serait régie par un contrôle permanent sur les individus ? Voulons-nous, pire encore, d'une civilisation où l'on obligerait tous les individus à se soumettre à des tests génétiques ? Je précise que des dizaines de millions de personnes sont soumises maintenant à des prélèvements à des fins de cartographie génétique totale de la population chinoise. Après le crédit social, on pourrait parler quasiment du génome social en Chine.

Nous devons nous tenir à égale distance de deux films de science-fiction.

D'une part, *Minority Report*, c'est-à-dire une société basée sur la surveillance absolue, totale et prédictive du comportement des individus. Ce n'est plus totalement de la science-fiction. Les forces de police, aux États-Unis et dans d'autres pays du monde, utilisent déjà des analyses *big data* pour pré-positionner les forces de police dans des endroits repérés comme ayant une forte probabilité de voir se produire des crimes ou des délits.

De l'autre, *Gattaca*, c'est-à-dire une société basée sur l'eugénisme et sur la génétique comme outil non seulement de traçage, mais également de contrôle et d'organisation sociale. Là encore, ce n'est plus tout à fait de la science-fiction. Aux États-Unis, la loi HR1313 a été présentée devant la Chambre des représentants. Elle avait pour but d'obliger à faire passer des tests à tous les employés des entreprises américaines à des fins de prévention des maladies. Les données auraient été détenues par les employeurs et les personnes qui refuseraient de se soumettre à ces tests auraient été sanctionnées à hauteur de 4 000 à 5 000 dollars par an. Cette loi n'est pas passée du fait de l'opposition des démocrates et, ensuite, du changement de majorité de la Chambre des représentants, mais elle illustre parfaitement cette tentation d'organisation sociale extrême, de rationalisation sociale extrême, de « solutionnisme technologique », pour reprendre l'expression d'Evgeny Morozov, de fascination pour l'efficacité technologique poussée à son extrême.

Puisque nous sommes en temps de pandémie, je rappellerai que des cabinets d'études sérieux avaient dit que le seul moyen de gérer à l'échelle mondiale une pandémie serait d'installer des capteurs de détection virale ou de menace biologique partout sur la planète pour en faire un réseau mondial qui détecterait les premières menaces où qu'elles apparaissent. L'auteur du rapport en question estimait que ce projet serait utile même si beaucoup de responsables politiques n'oseront jamais le mettre en œuvre parce qu'ils ne mettront pas l'intérêt de leurs citoyens devant leurs considérations politiques.

L'on sait que ce projet se heurterait à des objections sur le caractère liberticide de ce genre de surveillance totale et instantanée, mais ce serait quand même le plus grand marché jamais entrepris en matière de technologie. Il existe cette fascination pour des solutions

liberticides, c'est-à-dire qui considèrent que démocratie, droits de l'homme, liberté sont des variables d'ajustement.

J'ai plaisir à le rappeler ici même, au sein de l'Assemblée nationale, en période de pandémie, parce que malheureusement, cette tentation a souvent été exprimée dans la période récente, c'est-à-dire de considérer que les libertés peuvent être mises entre parenthèses. Cicéron disait : « En temps de guerre, la loi se tait ». En temps de guerre pandémique, la loi devrait se taire. Non ! Si nous avons une possibilité de développer une activité autonome, indépendante des grandes plateformes asiatiques et américaines, c'est en nous appuyant sur les erreurs récentes, les fautes récentes qu'elles ont commises. Je pense à deux événements en particulier.

Le premier est l'affaire Snowden, la révélation des liens existants entre les services de renseignements américains et en particulier la NSA (*National Security Agency*) avec ces grandes sociétés. L'on a vu qu'elle a été à l'origine de la remise en cause du transfert des données des Européens aux États-Unis. La conséquence première de l'affaire Snowden pour nous, Européens, en plus d'apprendre le détail du fonctionnement et du niveau de surveillance que pouvaient établir des agences de renseignement dans ces domaines a été que la Cour de justice de l'Union européenne, en 2015, a eu l'occasion de remettre en cause le *Safe Harbor*, le premier accord transatlantique sur le transfert des données des citoyens européens aux États-Unis.

Cet accord, je le précise, était utilisé par plusieurs milliers de sociétés aussi bien aux États-Unis que dans d'autres pays. Auparavant, l'on considérait que les données transmises aux États-Unis étaient protégées, étaient relativement sûres et l'on s'est rendu compte que ces données pouvaient non seulement être analysées, mais être transmises pour essayer d'aider telle ou telle société. L'on pourrait citer le conflit entre Boeing et Airbus, mais les exemples ont été nombreux. Une crise de confiance à l'échelle mondiale, une crise de confiance systémique était sur le point de se produire par rapport à l'utilisation massive de ces données par des plateformes.

L'Union européenne, mal lui en a pris, a renégocié en urgence un autre accord, le *Privacy Shield*, qui vient, le 20 juillet dernier, d'être remis en cause par la même Cour de justice de l'Union européenne pour les mêmes raisons. Au départ, c'était juste après le scandale de l'affaire Snowden. Par la suite, cela a été le scandale de l'affaire Cambridge Analytica, l'utilisation des données des réseaux sociaux (Facebook en l'occurrence) à des fins de manipulation politique. L'on s'est rendu compte que les données des Européens ne sont pas protégées quand elles sont transmises de cette manière, compte tenu, en plus, du fait que les lois américaines s'appliquent de manière extraterritoriale, c'est-à-dire en dehors du territoire américain à des sociétés américaines basées en Europe.

Je rappellerai, pour ceux qui l'auraient oublié, qu'en janvier 2017, c'est-à-dire quelques jours après avoir pris ses fonctions de président des États-Unis, un certain Donald Trump émettait une ordonnance (*executive order*) privant les citoyens non américains de toute forme de protection de la vie privée dans le cadre des lois américaines. C'est ce qui avait valu à l'époque une interpellation de la part du groupe article 29, c'est-à-dire les commissions nationales de l'informatique et des libertés (CNIL) européennes, qui s'étaient interrogées sur la pertinence du *Privacy Shield*. Je précise que les responsables de la CNIL en France n'ont jamais reçu de réponse des autorités américaines.

À l'évidence, nous avons péché par naïveté, pour reprendre le terme employé par Thierry Breton dans sa tribune récente. Je rappellerai un propos que nous objectaient souvent nos interlocuteurs du département d'État quand nous étions aux Nations unies : « Vous, les

Européens, vous ne savez que geindre. Vous n'avez pas d'industrie et la seule manière que vous trouvez de nous ralentir, ce sont les actions juridiques. » Il faut bien comprendre que ces propos n'ont pas été seulement prononcés par Donald Trump dans la période récente, mais également par Barack Obama en 2015 qui déclarait, devant un auditoire d'entrepreneurs américains : « Les préoccupations élevées des Européens en matière de protection des données personnelles n'ont pour but que de nous ralentir parce qu'ils n'ont pas d'industrie, parce qu'ils n'ont pas créé l'internet. »

Cela est faux, je le précise, l'internet a été créé sur la base de travaux qui ont été menés en France par un certain Louis Pouzin qui a été récompensé par la reine d'Angleterre pour sa contribution à la création de l'internet au travers de technologies qui ont été élaborées en France. Le web a été lui aussi inventé en Europe par un Européen, Sir Tim Berners-Lee. De la même manière, l'une des innovations majeures des technologies de l'internet, qui équipe plus de 90 % des serveurs dans le monde, Linux, a été inventée en Europe par un Européen.

Nous, Européens, avons laissé les fruits commerciaux, stratégiques de ces révolutions se faire réapproprier par des sociétés qui ont su en tirer des bénéfices. « Il est temps d'en finir avec la naïveté », disait Thierry Breton. Cela est vrai du point de vue de la régulation où, enfin, l'on parle de mesures antitrust de manière claire, l'on parle de démantèlement, on parle de bloquer les marchés, on parle d'empêcher des fusions. L'Europe a accepté le rachat de WhatsApp et d'Instagram par Facebook alors qu'elle aurait dû s'y opposer.

Je précise qu'au début des années 2000, l'Union européenne était capable d'empêcher des fusions, y compris entre sociétés américaines. General Electric et Honeywell par exemple n'ont pas pu fusionner leurs activités sur les moteurs d'avions à cause d'une action européenne. L'absence de stratégie et de politique industrielle française et européenne, le fait que les grands projets européens aient essentiellement servi de variable d'ajustement pour de grands groupes et n'aient pas permis de développer un écosystème de petites entreprises innovantes et surtout de le faire croître. Tout le monde parle de la *Start-up Nation*. Je préférerais que nous soyons une *Unicorne Nation* ou, mieux encore, une *Big Tech Nation*. Excusez-moi de parler en anglais, mais en gros, je préférerais que nous ayons la capacité à faire grandir ces sociétés hormis par le rachat ou l'expatriation.

Or, pour l'instant, les quelques sociétés qui ont pu émerger dans ces domaines sont, la plupart du temps, obligées d'envisager un rachat par des structures étrangères. Il existe des mécanismes auxquels se sont opposés certains de nos partenaires européens comme l'Angleterre dans le passé sur le *Small Business Act*, les Anglais refusant de toucher aux marchés publics au nom de la distorsion de concurrence.

Non, les Américains pratiquent une politique industrielle extrêmement agressive, extraordinairement interventionniste là où nous sommes spectateurs, alors que nous devons devenir acteurs pour, comme le rappelait l'excellente économiste italo-américaine Mariana Mazzucato, que l'État assume son rôle de stratège, voire assume son rôle d'entrepreneur. Tel était le titre de son livre : *L'État d'entrepreneur*. Rappelons par exemple que les technologies fondamentales utilisées aujourd'hui dans l'iPhone, pour quasiment la totalité d'entre elles, ont été développées sur des crédits fédéraux américains. L'internet le premier a été développé sur fonds fédéral militaire, mais l'on pourrait parler des écrans tactiles, des interfaces vocales, des interfaces en réalité augmentée, pratiquement toutes les technologies clés ont pu être développées parce que la puissance publique a largement investi dans leur développement, parce que la puissance américaine, depuis plus de cinquante ans, a développé un mécanisme appelé le *Small Business Act*, c'est-à-dire une loi orientant une partie significative de la commande publique vers des PME innovantes.

Nous devons urgemment réfléchir à ces mécanismes. À chaque fois, l'on nous oppose : « Non, de toute manière, des financements, il y en a. » Mais ce qui importe, ce n'est pas que le financement, c'est pour des entreprises européennes d'être en mesure d'avoir la possibilité de faire évoluer leurs produits face à des clients solvables, et ce dans les premiers temps de leur création. Le *Small Business Act* et les possibilités d'orienter et d'aider la recherche sur des secteurs stratégiques, c'est ce qu'ont fait les Américains. Ils continuent de le faire dans le spatial avec SpaceX, qui repose de façon très importante sur les commandes publiques de la NASA, mais cela est vrai de pratiquement toutes les entreprises en termes de défiscalisation. Je lisais un article récent sur les usines que Tesla va créer en Europe et qui seraient, pour beaucoup, financées indirectement par des crédits européens. Je crois que, là encore, il nous faut rompre avec la résignation passive par rapport aux choix technologiques dans ces domaines.

Je parlais de sécurité sanitaire et de l'importance qu'elle pourrait avoir au niveau européen. Avec la pandémie, l'on voit bien que les données autour de la santé qui sont des données sensibles au sens de la CNIL deviennent extraordinairement stratégiques. Un projet, décidé un peu avant la pandémie, a été mis en place et accéléré pendant la pandémie : il s'agit du projet de plateforme des données de santé mis en place par le ministère de la santé. Ce projet réunit à lui tout seul tous les paramètres qui ont dysfonctionné dans les politiques industrielles en Europe et en particulier en France.

Je rappelle sa genèse. Ce projet est né à la suite du rapport de Cédric Villani sur l'intelligence artificielle qui préconisait que soient développés des outils d'intelligence artificielle en santé et, pour cela, de réunir les données de santé dans le cadre d'une plateforme, le *Health Data Hub*. J'en parle pour avoir travaillé dans les services du Premier ministre sur les questions d'administration électronique il y a fort longtemps. Quand on a un projet aussi stratégique, l'on doit s'interroger sur son impact sur l'écosystème technologique et sur ses missions à long terme. Or les deux n'ont pas été faits correctement.

D'une part, ce projet a été confié, pour son hébergement, à Microsoft, ce qui a suscité de nombreuses critiques et interrogations de professionnels de la santé. L'ancien président du comité d'éthique y a vu un cadeau insigne fait à la société Microsoft. Au-delà, l'on y a vu un risque sur l'évolution même du secteur de la santé.

Si vous me permettez une parenthèse dans la parenthèse, aujourd'hui, beaucoup de gens s'interrogent sur le devenir des GAFAM en disant : « Ils ont pu exercer leurs muscles sur des secteurs que l'on identifie assez bien, la publicité, les transports, *etc.* Les segments de croissance prioritaires pour ces sociétés aujourd'hui sont les services financiers et le secteur prudentiel, c'est-à-dire tous les services de banque et d'assurances. » Plus que de devenir des acteurs de la santé au sens traditionnel comme le sont les acteurs pharmaceutiques ou les acteurs du soin, ces sociétés qui ont acquis une somme considérable de données sur les individus sont capables de profiler les risques.

Qu'est-ce qu'un assureur ? C'est d'abord un acteur qui est capable de mesurer les risques pour chaque individu. Les grandes plateformes (Facebook, Google, Apple) sont en mesure de participer à l'analyse de données extraordinairement précises sur les individus et donc de proposer des assurances hyper individualisées, ce qui pour nous, Européens, et surtout pour nous, Français, semble très éloigné de notre modèle social de couverture mutualisée du risque. Vu d'un acteur technologique, il s'agit d'une opportunité considérable. Je recommande un extraordinaire rapport qui a été établi par la branche recherche de Goldman Sachs qui évoquait l'introduction des objets connectés dans le champ de la santé comme un vecteur possible d'économies de plusieurs centaines de milliards par an pour le système de santé

américain. Ce rapport montrait que la prévention en matière de santé pouvait devenir un outil d'économies considérables, et donc de bénéfices considérables pour les acteurs en question.

Je reviens sur la plateforme des données de santé. Nous ne devons pas nous préoccuper seulement des gains immédiats, mais nous devons avoir une vision stratégique sur ce que devient le secteur santé qui est, on le voit bien en période de crise pandémique, l'un des secteurs stratégiques pour l'ensemble des acteurs européens. Si l'on assistait à une « ubérisation » de l'assurance santé (je précise que Google a annoncé il y a quelques semaines sa première initiative d'assurance santé aux États-Unis et l'on ne doute pas qu'il ait l'intention de la déployer dans d'autres régions du monde), il faut se poser la question de l'évolution de ce secteur, de notre volonté ou pas d'empêcher que se mettent en place des solutions de contrôle, de monitoring des activités comme le font les objets connectés aujourd'hui, voire de maternage, pour inciter les individus à modifier leurs comportements.

L'on est capable de faire en sorte que ces technologies accompagnent les individus pour modifier leurs comportements. C'est déjà le cas d'un point de vue idéologique sur les réseaux sociaux : l'on se rend compte que l'on est capable de modifier et d'accentuer certaines réactions en fonction de l'état de l'humeur ou de l'histoire personnelle de chaque utilisateur. En matière de santé, il s'agit un peu de la même idée.

Comment devons-nous nous situer, nous Européens, dans l'évolution de ces technologies ? L'idée est de faire en sorte d'aider à développer des solutions éthiques, des solutions qui soient en accord avec les principes et valeurs des Européens. Maîtriser notre destinée numérique, c'est aussi maîtriser notre destinée politique dans ces domaines et essayer de faire en sorte de développer une voie alternative aux exemples de dérives sino-américaines. Récemment, lors d'un débat sur la 5G, un industriel déclarait : « Les Européens sont absents de ce débat ». Je lui répondais : « Non, les Européens sont présents dans ce débat : ils sont les proies. » Je précise que le ministre américain de la justice, M. William Barr, a eu l'occasion, dans le cadre de ce conflit avec la société Huawei, qui est l'un des grands acteurs de la 5G, de dire : « Nous devons, avec des sociétés alliées, prendre des participations majoritaires dans deux acteurs européens, Nokia et Ericsson, parce qu'ils possèdent un portefeuille de brevets important dans ces domaines. » D'alliés traditionnels, nous sommes devenus les proies que l'on vient dépecer pour renforcer la puissance industrielle américaine. Est-ce la destinée de l'Europe ? J'espère que non. Sommes-nous capables d'aider à développer des acteurs européens qui restent européens et qui ne sont pas soumis à des diktats sur le modèle économique comme le sont les diktats mis en place par Facebook, Google, Amazon ? Voilà la vraie question pour les temps qui viennent.

Je parlais de quelques mesures de régulation que sont le *Small Business Act*, l'aide à la commande publique, les actions de stratégie industrielle. Une autre action de coordination de la gouvernance des technologies a été prise aux États-Unis : la création, sous Barack Obama, d'un *chief technology officer* pour l'administration fédérale américaine. Il s'agit d'un coordinateur fédéral pour les technologies de l'État qui répond directement à la Maison-Blanche. Je crois qu'au niveau français et européen, nous aurions grand avantage à avoir ce type de fonction transversale qui analyse les technologies non pas seulement sur le plan industriel ou sur le plan des services rendus aux citoyens, mais bien sur le plan de leurs impacts sociétaux, culturels, sur l'ensemble de la population.

Je rappellerai que la ville de Toronto avait passé un accord avec Sidewalk Labs, une filiale de Google, pour gérer les technologies de la ville intelligente de Toronto. Plus les citoyens de Toronto ont été informés du détail des opérations qui se mettaient en place, plus ils se sont rendu compte que cela ressemblait au crédit social chinois, c'est-à-dire la notation systématisée, l'obligation de transparence par rapport aux données personnelles, les sanctions

pour les personnes qui n'obtempéreraient pas. S'est posée une question de souveraineté au sens premier. Les citoyens de Toronto ont dit : « Nous n'avons pas élu le patron de Google, il n'a pas à diriger nos vies. » Un mouvement d'opinion massif s'est mis en place et, en mai dernier, la filiale de Google en question a annoncé l'arrêt total de ce projet. L'on voit bien le risque du micro-profilage que j'évoquais tout à l'heure, c'est-à-dire l'acquisition d'une grande quantité d'informations sur les individus qui permet par la suite d'appuyer sur telle ou telle tendance pour les manipuler.

C'est ce que dit très bien l'excellente Shoshana Zuboff, professeure à Harvard, dans *L'âge du capitalisme de surveillance*, livre qui est traduit en français depuis quelques jours. Aujourd'hui, il n'est plus question simplement d'orienter le comportement commercial des individus. Le but est de modifier leur état d'humeur, de renforcer certaines convictions, de modifier leur comportement politique. Elle dit : « Nous croyons que nous cherchons avec le moteur de recherche Google, alors que c'est lui qui cherche en nous. » Toutes les informations que l'on donne à un moteur de recherche ne sont jamais perdues. Toutes les informations qui sont dans un réseau social sont rassemblées, traitées, échangées par des courtiers en données (« *data brokers* ») et constituent des profils d'une extraordinaire précision sur les individus. Devant le Congrès américain, Mark Zuckerberg a été obligé de reconnaître que Facebook récupérait, stockait et analysait des données sur des personnes qui n'étaient même pas des abonnés Facebook (« *shadow profiles* ») pour être en mesure d'étendre le niveau d'analyse et donc de recommandation publicitaire de Facebook, y compris de données médicales.

Je crois que nous devons nous poser des questions bien au-delà des simples questions industrielles, économiques traditionnelles. Ce dont relève aujourd'hui le numérique, c'est véritablement de questions politiques au sens profond, c'est-à-dire d'orientation générale de l'activité de notre société pour les temps à venir. C'est pour cela que nous devons aussi développer dans le même temps des régulations et une politique industrielle forte pour développer nos propres acteurs avec leurs propres orientations stratégiques.

M. Philippe Latombe, rapporteur. Merci pour ce propos introductif. Nous avons en Europe et en France en particulier des très bons industriels dans le domaine de la reconnaissance faciale. Nous avons certainement parmi les meilleurs dans ce domaine.

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Je crains que les Chinois ne soient meilleurs.

M. Philippe Latombe, rapporteur. Les Chinois sont meilleurs parce qu'ils ont une partie de la « bibliothèque », ce que nous n'avons pas forcément. En France et en Europe, la reconnaissance faciale suscite un débat : faut-il l'autoriser ou l'interdire ? Nous sommes dans une espèce d'entre-deux où rien n'est autorisé et rien n'est interdit. Le fameux Livre blanc de l'Union ne l'a pas vraiment traité. Nous avons des questions qui se posent aujourd'hui, notamment en France. Vous avez parlé des valeurs et du « solutionnisme technologique ». La reconnaissance faciale est à la croisée de ces deux points. Qu'en pensez-vous ? L'Europe doit-elle interdire la reconnaissance faciale ?

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Très peu de technologies sont intrinsèquement négatives. Je pourrais citer par exemple les technologies de *deepfake* qui permettent de déshabiller des individus de manière à les gêner voire à faire pression sur eux ou à les menacer.

Les algorithmes de reconnaissance faciale peuvent être sujets, comme ils l'ont été souvent aux États-Unis, à des discriminations et donc favorisent une reconnaissance efficace

des Caucasiens, c'est-à-dire des blancs, à la différence des Noirs ou des Afro-américains, où l'on a eu des cas d'arrestations à cause d'une reconnaissance faciale erronée.

Tout dépend de la manière dont ces technologies sont conçues. Je parlais tout à l'heure des systèmes bancaires. Apple, qui est devenue une banque en s'alliant avec Goldman Sachs, a mis en place des systèmes de crédit. Quelqu'un a remarqué qu'à revenu égal, une femme avait une espérance de crédit dix fois inférieure à un homme sur la plateforme d'Apple. L'on s'est rendu compte qu'il existait un biais, une discrimination algorithmique au sein de la plateforme. Cela a même été confirmé par le cofondateur d'Apple, Steve Wozniak.

Je crois que les technologies, y compris les technologies de reconnaissance faciale, mais aussi l'ensemble des technologies militaires (je rappelais les liens historiques entre la Silicon Valley et les financements militaires : beaucoup de projets initiaux de la Silicon Valley ont été à orientation militaire dans pratiquement tous les secteurs) peuvent être utilisées à bon ou à mauvais escient.

Comment ces technologies interviennent-elles dans le champ social ? Voilà ce qui me préoccupe. Va-t-on vers *Minority Report* avec une reconnaissance faciale généralisée, avec des risques de contrôle qui s'étendent au-delà du raisonnable ? C'est tout le débat. Que ces technologies puissent être utiles ou utilisables, bien sûr. Qu'elles doivent être généralisées au point que l'on rentre dans un système de surveillance totale comme c'est le cas en Chine, non. L'une des sociétés les plus valorisées dans le domaine de l'intelligence artificielle en Chine est justement une société sur la reconnaissance faciale, dont le principal client est le gouvernement chinois. Quelles limites donnons-nous à ces acteurs ? Quel modèle économique développe-t-on à partir de ces technologies ? Est-ce un modèle de surveillance absolue ? D'après le *Financial Times* qui a mené une enquête, certains *data brokers* réunissent déjà plusieurs centaines de millions de profils différents et plusieurs dizaines de milliers de paramètres par individu. Je pense qu'il est des modèles économiques qui sont toxiques. Avec l'affaire Cambridge Analytica, on a vu comment une frange de l'électorat était capable de basculer avec des campagnes de manipulation de masse hyper individualisée.

Il ne faut pas considérer qu'une technologie est mauvaise en elle-même sauf rares exceptions, mais considérer qu'une technologie doit être utilisée en ayant conscience de ce qu'elle peut générer. Quand on fait des tests génétiques massifs, on sait très bien que cela peut générer d'autres formes de surveillance encore plus inquiétantes. Quand on fait de la reconnaissance faciale à raison de plusieurs centaines de millions de caméras sur le territoire chinois par exemple, on sait très bien que cela correspond à une forme de dictature numérique, avec l'autosurveillance des individus et l'autocensure des individus, la surveillance par l'État, l'ensemble étant mis en œuvre avec des systèmes de reconnaissance faciale aussi. Là encore, c'est dans la manière dont ces technologies seront déployées que risquent de se trouver des problèmes ou des questions politiques et philosophiques sur le devenir de nos sociétés.

M. Philippe Latombe, rapporteur. Je vous pose une question que pose mon collègue Pierre-Alain Raphan. À votre avis, quelles actions doit-on mener à destination des citoyens pour les sensibiliser aux enjeux de cette économie de l'attention ? Que doit-on faire pour susciter une prise de conscience ? Nous avons quand même l'impression d'un manque d'information quant aux enjeux de cette économie de l'attention.

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Vous avez parfaitement raison et vous remercierez votre collègue, le député Raphan, de cette question. Je crois qu'il est important de sensibiliser et d'éduquer. C'est l'ancien délégué aux usages de l'internet qui vous parle.

De manière générale, pour être efficace, il faut agir sur trois volets : l'éducation/sensibilisation, la régulation des technologies et la régulation juridique. Il ne faut pas faire reposer sur le citoyen l'essentiel du poids. Je crois qu'il est important d'informer le citoyen pour qu'il puisse constituer une force de réaction. Je vous parlais de la réaction citoyenne à Toronto, une réaction que je trouve remarquable. Il faut qu'il y ait une sensibilisation suffisante dans ces domaines.

Pour l'instant, nous en sommes au tout début. Il est évident que les plateformes dont nous parlons (Facebook, Google, *etc.*) ne perdront pas d'emblée des centaines de millions de leurs utilisateurs. Il faut arriver à réguler leurs comportements les plus toxiques et à faire en sorte que les acteurs de ce secteur, y compris les investisseurs, perçoivent les risques. Ils commencent à les percevoir.

Ainsi, la société Palantir qui fait le *big data* pour les services de renseignement américains a, malheureusement, été choisie à deux reprises par la DGSI (direction générale de la sécurité intérieure) pour gérer les données antiterroristes et a même proposé gratuitement ses services à l'AP-HP (Assistance publique-Hôpitaux de Paris) pour la gestion des données covid. L'AP-HP a refusé, mais nos voisins britanniques du NHS (*National Health Service*), eux, ont accepté. Cette société est rentrée en bourse il y a peu. Dans son dossier de présentation, elle indiquait : « Les modifications du paysage de la régulation pourraient être amenées à remettre en cause la nature même de notre modèle économique. » Ils ont raison !

Aux États-Unis, la majorité démocrate de la Chambre des représentants a émis un rapport très dur sur ces plateformes, et en particulier sur les aspects antitrust. Plus près de nous, la Chambre des communes britannique a qualifié dans un rapport ces plateformes de « gangsters numériques qui subvertissent la démocratie ». Je crois qu'il est temps de faire en sorte que l'écosystème, y compris les investisseurs, soit conscient qu'il existe un risque. Je pense qu'il s'agit d'un moyen de pression important, en plus des actions antitrust, en plus de l'ensemble des actions de régulation.

Je crois que la sensibilisation des citoyens est importante, mais ne sera pas suffisante. Elle doit être complétée par la régulation technologique et la régulation juridique. Le règlement européen sur les données est maintenant exporté dans de très nombreux pays, bien au-delà de l'Europe. Même les Chinois s'appuient sur le règlement général sur la protection des données (RGPD) pour développer leur propre législation sur la protection des données ! Nous devons aller vers une meilleure compréhension par les citoyens, par les responsables, par les régulateurs, par les législateurs. C'est l'ensemble de ce spectre d'actions qui doit être mené dans les temps à venir.

M. Philippe Latombe, rapporteur. Vous avez évoqué le *Small Business Act* et les capacités que les pouvoirs publics peuvent avoir non pas en accordant des subventions, mais en fournissant des contrats aux entreprises. Vous avez parlé du RGPD et de la réglementation. Vous avez évoqué les décisions de justice *Schrems I* et *Schrems II* très récemment. Je ne vous pose pas la question : y aura-t-il un *Privacy Shield* 2 qui ferait un *Schrems III* ? Quelles seraient, dans les mois ou l'année qui vient, les mesures à prendre au niveau européen pour essayer de mettre ces barrières ? Si vous aviez une baguette magique et que vous étiez à la place de l'ensemble des décideurs, que proposeriez-vous ?

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Si j'avais une baguette magique, j'empêcherais que l'on mette de côté les travaux de Louis Pouzin il y a cinquante ans pour aider à créer un internet européen.

M. Philippe Latombe, rapporteur. Si vous aviez une baguette magique qui fonctionne pour l'avenir et pas pour le passé, que feriez-vous ?

M. Bernard Benhamou, secrétaire général de l'Institut pour la souveraineté numérique. Je trouverais parfaitement regrettable que nous soyons soumis à un *Schrems III*, c'est-à-dire que l'Union européenne ne retienne rien des leçons du passé. Il est temps de mettre un terme à la naïveté, c'est-à-dire qu'il faudrait localiser les données en Europe (*data sovereignty*, *data localization* ou *data residency*). Les données des Européens doivent être traitées en Europe par des acteurs européens. Quand je dis des acteurs européens, pas des faux-nez, de vrais acteurs européens dont le siège et le quartier général sont en Europe. Certains disent, y compris dans l'exécutif, qu'une société comme Microsoft est une société européenne ! La définition est tangentielle parce que, malheureusement, le droit américain s'applique y compris pour les données stockées en Europe.

Nous avons donc besoin d'établir de nouveaux principes. Je précise que les acteurs américains avaient déjà anticipé ce durcissement des législations en créant des *data centers* en Europe. Il faut aller beaucoup plus loin. Je sais qu'une proposition de résolution européenne vient être proposée au Sénat par Mme Morin-Desailly sur ces questions, sur le fait d'obliger à traiter des données sensibles des Européens en Europe par des acteurs européens. Je pense qu'il faudra modifier nos textes. Il en va de notre sécurité nationale et de notre souveraineté. La sécurité nationale ne faisant pas partie des prérogatives sur lesquelles l'Union européenne a à se prononcer, il serait tout à fait possible de modifier les textes de manière à imposer que les sociétés traitant des données sensibles classiques (données de santé, politiques, ethniques, religieuses, philosophiques, sexuelles) et des données qui en apparence ne sont pas sensibles, mais qui le deviennent soient européennes. En analysant des données sur le comportement d'un individu, par exemple sur son périmètre de marche, l'on est capable de prévoir s'il va avoir des maladies ou pas. En analysant son comportement avec la montre connectée d'Apple, l'on peut prévoir les crises de panique.

Il faut bien comprendre qu'il y aura en même temps à déterminer une stratégie industrielle pour faire en sorte que les Européens développent leurs marchés et leurs technologies et évitent de transférer des données à l'étranger, sur lesquelles ils n'ont plus de contrôle. Je rappelle que les *data brokers* qui échangent entre eux des données, qui vendent parfois des profils à des administrations, sont une sorte de trou noir pour la régulation sur les données. Les acteurs qui ont développé le RGPD disent que cela ne tiendra pas.

Il faut aider à créer un cadre beaucoup plus protecteur pour les données et, en amont de la collecte, se poser la question de savoir si certaines données ne doivent pas faire l'objet d'une extraction, ne doivent pas être traitées. Il s'agit d'une vraie question pour les temps qui viennent. À partir de quand devra-t-on empêcher que certaines données puissent être traitées ? Des chercheurs viennent de publier dans *Le Monde* d'aujourd'hui une critique sur les questions de sécurité concernant le *Health Data Hub* en disant : en concentrant les données à un seul endroit, l'on crée un point de vulnérabilité important, un point d'attaque possible. De nombreuses questions s'entremêlent autour de cela, mais la principale des baguettes magiques, c'est qu'il y ait une prise de conscience parmi l'ensemble des citoyens, des acteurs et des régulateurs dans ces domaines. Nous n'en sommes qu'au tout début.

M. Philippe Latombe, rapporteur. Merci beaucoup.

Audition, ouverte à la presse, de M. Stéphane Séjourné, député européen, rapporteur sur un cadre d'aspects éthiques en matière d'intelligence artificielle, de robotique et de technologies connexes
(5 novembre 2020)

Présidence de M. Jean-Michel Mis, vice-président.

M. Philippe Latombe, rapporteur. Je suis heureux d'accueillir Stéphane Séjourné, qui est député européen, qui a remis en octobre dernier un rapport sur les droits de propriété intellectuelle pour le développement des technologies liées à l'intelligence artificielle (IA). Comme vous le savez, la mission d'information porte sur les moyens de bâtir et de promouvoir la souveraineté numérique française et européenne. Dans le cadre de nos travaux, nous sommes évidemment particulièrement sensibles à l'actualité européenne dans le domaine du numérique. Nous avons d'ailleurs initié cette mission en rencontrant, lors de la Paris Cyber Week, Mme Mariya Gabriel, commissaire européenne chargée de l'innovation, de la recherche, de la culture, de l'éducation et de la jeunesse.

Nous poursuivons donc aujourd'hui notre travail de réflexion collective avec un représentant du Parlement européen, que je remercie très vivement d'avoir accepté notre invitation. Je crois qu'il est important que nous puissions dialoguer plus fréquemment, en tant que parlementaires, avec le Parlement de Strasbourg. Je souhaite que l'audition de ce jour nous permette de comprendre de quelle façon la souveraineté est envisagée, promue et défendue au sein de l'Union européenne. Je pense également qu'il serait utile de faire un point d'actualité sur les principaux dossiers numériques de l'Union européenne, en particulier en ce qui concerne les stratégies de la donnée et de l'intelligence artificielle, sujets sur lesquels vous êtes très engagé.

Je voudrais en premier lieu vous interroger de façon plus précise sur le sens de la notion de souveraineté numérique. Ce concept, rapproché parfois de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et à ne pas subir les contraintes imposées par certains acteurs publics (États) ou privés (GAFAM). De quelle façon envisagez-vous cette notion, et comment est-il possible de l'articuler avec des solutions concrètes en France et en Europe ? Nous sommes par ailleurs très intéressés par la vision que les autres pays européens ont de cette idée, de façon à décentrer au maximum notre regard de parlementaires français.

Je voudrais également revenir avec vous sur les enjeux économiques et technologiques de la souveraineté numérique. Nous le voyons en ce moment même : l'économie numérique fonctionne sur le principe selon lequel « *the winner takes all* ». Les GAFAM disposent d'un pouvoir de marché sans précédent, dans un nombre croissant d'activités. Les acteurs alternatifs européens ont beaucoup de mal à venir les concurrencer efficacement. La régulation du numérique, *via* le *Digital Services Act* (DSA), d'une part, et le maintien d'une dynamique d'innovation technologique en Europe d'autre part sont donc deux sujets sur lesquels nous aimerions vous entendre.

Nous souhaiterions également disposer d'un éclairage sur les enjeux et les débats autour de l'aspect éthique de l'intelligence artificielle, de la robotique et de ses technologies connexes, et sur la stratégie européenne en matière de données. Nous savons en effet que la présentation du *Data Government Act* par la Commission européenne devrait avoir lieu dans les prochains jours.

Enfin, la souveraineté numérique, c'est également la cybersécurité et la cyberdéfense, et donc notre écosystème public et privé. Selon vous, comment la France et l'Union européenne pourraient s'affirmer dans ces domaines ? Quels sont actuellement nos atouts et nos faiblesses pour développer une véritable industrie européenne de la cybersécurité ?

M. Stéphane Séjourné, député européen. Merci pour cette initiative. Il est en effet important de pouvoir échanger entre la représentation nationale et les parlementaires européens – nous devrions nous aussi être capables de vous auditionner sur un certain nombre de points, ce qui est envisagé par le Parlement, même si les conditions sanitaires nous entravent sur ce point. J'en profite pour souligner que le Parlement européen dispose d'outils permettant de continuer à travailler à distance, de façon décentralisée et dématérialisée, avec la possibilité de voter et de suivre des commissions à distance. Je constate que l'Assemblée nationale dispose également de ces outils, ce qui me semble positif pour notre pratique.

Sur les questions que vous avez évoquées, la souveraineté européenne passe d'abord par la capacité à agir, en défensif ou en offensif, à prévoir sa propre régulation dans le cadre institutionnel actuel, mais également à répondre à un certain nombre d'enjeux communs à l'ensemble des États membres. Au sein de tous les principaux groupes politiques européens – les Verts, le PPE, Renew Europe et les Socialistes –, on constate la même volonté de construire un modèle autour de cette souveraineté numérique, qui ne serait ni le modèle chinois ni le modèle américain, et d'exporter par la suite ce modèle comme une référence d'un point de vue éthique, moral et industriel. Avant d'en arriver là, il existe un sujet primordial, en l'occurrence la stratégie européenne des données : en effet, les données sont le « carburant » de tout ce qui émergera en termes de souveraineté numérique européenne, ce qui pose la question de notre capacité à organiser la collecte, le traitement et l'utilisation des données. Cet écosystème ne pourra être établi qu'à partir du moment où ce carburant sera réglementé, avec une collecte dont les modalités auront été harmonisées chez les 27. Cet enjeu est l'enjeu premier de toute la stratégie de souveraineté. Thierry Breton est aujourd'hui en pointe sur ces sujets : la Commission souhaite en premier lieu entrer sur cette question avant de développer l'ensemble des autres enjeux.

Parmi ces autres enjeux, nous avons notre modèle européen sur l'intelligence artificielle, modèle sur lequel nous travaillons actuellement. Nous avons choisi d'entrer par plusieurs biais qui, aujourd'hui, sont des angles morts de la réglementation européenne : le modèle éthique de l'intelligence artificielle, la question de la responsabilité – et donc de la responsabilité civile, avec notamment la question de la voiture autonome – et la question de la propriété intellectuelle. En effet, de plus en plus d'œuvres ou de productions pourraient être réalisées par l'intelligence artificielle de manière autonome, ce qui pose la question de la propriété intellectuelle pour toutes ces créations qui sont le fruit de l'intelligence artificielle. Aujourd'hui, les cas spécifiques sont peu nombreux, mais nous savons que ce domaine est appelé à grandir, et il nous manque un cadre réglementaire européen sur ces questions.

Un troisième enjeu, à mon sens, concerne la souveraineté et la protection de notre démocratie. Il s'agit de la pierre angulaire de ce que l'Europe peut protéger et organiser : c'est notamment la question de l'ingérence dans les élections. Il y a consensus, au Parlement européen, pour réfléchir à nos modèles de protection des démocraties. J'ai beaucoup voyagé à l'est de l'Europe, dans des pays qui ont plus d'expérience que nous en cybersécurité, en cyberdéfense et en ingérences politiques, de la part notamment de la Russie : force est de constater que nous avons d'importants progrès à faire sur ce sujet, qui est un sujet européen. Ce sujet doit permettre à l'Union européenne de développer un modèle de protection pour les États membres qui en font la demande, afin de les protéger contre toute forme d'ingérence, notamment électorale. Il convient également de tenir compte de la question du terrorisme, du

DSA, de la régulation des contenus haineux : ce sujet sera traité au Parlement, dans la mesure où, le 2 décembre, la Commission devrait nous proposer sa première feuille de route sur le DSA. Le DSA est l'actualisation de la directive sur le commerce électronique « e-commerce », avec de plus grandes ambitions. En France, nous avons quelques enjeux d'ordre économique : certains pays veulent en effet revenir sur le copyright, qui constitue une vraie victoire française. Il y aura donc des aspects défensifs, dans ce nouveau texte, et nous devrons collectivement y prendre garde – l'Assemblée nationale pourra nous aider sur ce plan. D'autres enjeux sont à développer, comme la régulation des contenus haineux, avec la mise en place d'une « loi Avia » au niveau européen, loi qui sera beaucoup plus efficace si un compromis est trouvé au sein de trois groupes politiques, qui sont très clivés en leur sein. Il s'agit d'ailleurs davantage d'une question culturelle que d'une question politique, avec des différences entre les pays nordiques, pays les plus libéraux, et les pays plus régulateurs. Il conviendra de trouver un compromis, ce qui sera relativement complexe.

Tel est aujourd'hui notre chantier, qui est donc très vaste à l'échelle européenne.

M. Jean-Michel Mis, président. Je commencerai par vous poser quelques questions pour parler des logiques de coopération entre les différents pays et États membres de l'Union européenne. Vous venez d'évoquer, au-delà des enjeux technologiques, des enjeux qui seraient de nature culturelle ou qui auraient trait aux différences d'appréhension des différents pays européens. De ce point de vue, pensez-vous que les élections américaines sont de nature à polariser les positionnements des pays européens, notamment dans leur relation aux GAFAM ou, à l'inverse, dans leur capacité à faire davantage de coproductions de type GAIA-X sur le *cloud* ? Par ailleurs, les enjeux de régulation et de normalisation sont importants dans le cadre de la directive DSA ou d'autres directives qui sont en cours d'évaluation, comme la directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dite « NIS » (*Network and Information System Security*) sur les fournisseurs de services essentiels. Pensez-vous que nous en fassions suffisamment sur ces enjeux, qui permettraient peut-être à l'Europe d'imposer des standards et d'être, non sur des logiques protectionnistes à l'égard de l'adressage du marché européen par la Chine ou les États-Unis, mais davantage dans une forme de régulation nouvelle, régulation qui est à construire et qui permettrait de trouver des solutions de résilience qui seraient plus favorables à notre écosystème européen ?

M. Stéphane Séjourné, député européen. En ce qui concerne les élections américaines, il convient de faire preuve d'objectivité : la victoire de Donald Trump a beaucoup aidé à la construction européenne, et a permis à l'Europe de prendre conscience qu'elle devait construire par elle-même un certain nombre d'axes de souveraineté qui manquaient à sa politique. Je le vois régulièrement au Parlement européen : les décisions du Président américain et son accélération vers l'unilatéralisme ont offert à l'Europe l'occasion d'une prise de conscience sur tous ces aspects. C'est vrai sur le numérique, mais pas seulement : en matière de défense – j'étais avec le Président de la République dans les pays baltes il y a peu –, nous entendons aujourd'hui des discours sur la construction de la défense européenne que nous n'aurions jamais entendus il y a encore cinq ans. La situation politique des États-Unis a donc permis à l'Union européenne de se reconstruire et de prendre conscience de la nécessité de travailler ces aspects, et de ne plus s'appuyer sur l'allié américain, qui avait décidé de ce repli depuis la présidence Obama. Je ne vois d'ailleurs par pourquoi cette tendance s'inverserait, même en cas de victoire de Joe Biden. Il existe donc un risque, au moment de l'alternance entre Républicains et Démocrates aux États-Unis, qu'un certain nombre de chantiers qui avaient été construits en réaction à la politique américaine soient ralentis ou abandonnés avec la volonté de retisser un lien transatlantique. Cette volonté ne doit pas s'opposer à ce qui a pu être construit dans le cadre de la prise de conscience européenne autour des valeurs de

souveraineté, qu'elle soit démocratique, économique ou numérique – sachant que nous faisons face à la problématique des GAFAM et aux enjeux entre l'Europe et les États-Unis autour de leur taxation. Tous ces éléments nécessitent donc une grande vigilance et une grande détermination, afin de faire prendre conscience aux dirigeants européens et à nos collègues députés européens, notamment dans un certain nombre d'États qui ont eu des liens particuliers avec les États-Unis et l'Organisation du traité de l'Atlantique Nord (OTAN), qu'une éventuelle alternance ne devrait pas changer notre ambition en la matière.

Sur les aspects régulation, le modèle européen n'est ni américain – les États américains tâtonnant eux-mêmes dans la façon de réguler le numérique et les nouveaux usages – ni chinois sur le volet éthique. Nous voulons en effet créer un standard européen qui permette à la fois le business, le développement des technologies, l'innovation, au service d'un modèle plus durable. Cette standardisation, que nous souhaitons la plus commune possible, nécessitera une politique de développement, dans une Europe géopolitique, ce qui suppose d'avoir la capacité d'exporter le modèle et d'imposer ses standards. Sur le volet éthique, notamment, il sera nécessaire de regarder les applications à risque et celles qui ne le sont pas, en particulier dans l'intelligence artificielle, afin de leur appliquer un certain nombre de standards en matière de libertés publiques et de contrôle en transparence. La transparence, c'est la confiance, en particulier dans un moment où il existe beaucoup de défiance à l'égard du politique, du scientifique et des nouvelles technologies. De fait, la transparence du modèle européen que nous souhaitons construire sera importante. Tous ces aspects de régulation ne doivent pas handicaper le business, le développement technologique, la capacité à innover ou la croissance des entreprises dans ces secteurs. L'objectif est d'être capable d'exporter ce modèle proprement européen, dans ses dimensions sociales, éthiques et environnementales.

M. Jean-Michel Mis, président. Merci pour ces premières analyses. Je vous propose un premier tour de table pour permettre à nos collègues de poser leurs questions.

M. Stéphane Séjourné, député européen. Je suis également preneur de vos remarques sur les textes à venir.

M. Éric Bothorel. En matière de souveraineté, j'ai eu à traiter cet été un dossier difficile, en l'occurrence celui de Nokia. J'aurais pu espérer, de la part de l'Europe, une position beaucoup plus ferme quant à la manière d'agir vis-à-vis d'un groupe européen, afin d'éviter qu'il délocalise son implantation en France au profit de la Pologne, du Canada et de l'Inde. J'avais interpelé le commissaire Breton, au titre de la commission des affaires européennes de l'Assemblée nationale, et je n'étais pas tout à fait satisfait de la réponse. Je ne pense pas que notre administration soit de nature à prendre des positions qui furent celles de Donald Trump, en contraignant à une reprise par une entreprise nationale comme ce fut le cas pour TikTok. Entre les deux positions extrêmes que sont le Far West américain et le Big Brother chinois, il doit exister une voie intermédiaire, plus ferme, de façon à faire en sorte qu'un *pure player* européen puisse s'exprimer au niveau mondial, avec des règles du jeu qui soient favorables à l'Europe qui l'accompagne, qui l'a vu naître et qui continuera de l'accompagner.

M. Denis Masséglia. Il y a quelque temps, je me suis déplacé aux États-Unis pour comprendre pourquoi la France, qui compte tant d'ingénieurs capables d'inventer de nombreux logiciels et de nouvelles idées, n'est pas capable de les mettre en œuvre pour créer de la richesse – raison pour laquelle nos ingénieurs et nos entreprises partent aux États-Unis. La réponse, pour les entreprises, tient au marché : le marché américain est important, et son développement nécessite autant d'énergie que le développement du marché français, du marché belge ou du marché allemand. Il convient donc de créer un marché unique européen permettant aux logiciels d'être vendus facilement, sans le blocage des différents pays. Cet objectif est difficile à atteindre, ne serait-ce que parce que nous parlons tous des langues

différentes. Pour faire émerger des champions européens, nous devons construire un écosystème permettant aux entreprises de se développer à partir de notre territoire européen. Quel est votre avis à ce sujet ?

Mme Nathalie Serre. Vous avez parlé de souveraineté numérique européenne, en considérant que le point névralgique était la stratégie des données. Or, avant même ce sujet, il me semble qu'il convient d'aborder la question de la consommation des ressources : électricité, climatisation, langage, base de données... Un travail est-il mené sur ces sujets ? Existe-t-il une stratégie européenne sur le langage qui sera utilisé ? Comment les ressources seront-elles utilisées ? Pour répondre au défi qui est devant nous, il convient de traiter ces sujets d'organisation matérielle avant d'avancer à l'étape suivante.

M. Stéphane Séjourné, député européen. Nous avons, en Europe, un problème de fragmentation du marché sur le numérique. En France, nous sommes très bons sur la recherche, mais moins bons sur les applications et la transformation de la recherche – d'où le travail mené par la Commission européenne sur la chaîne de valeur intégrée, de la recherche fondamentale jusqu'à l'application du quotidien. L'Europe se doit d'identifier le degré d'expertise de chaque État membre et de travailler à une régulation intégrée sur ces sujets. C'est notamment valable pour la partie 5G mentionnée par Éric Bothorel. Je suis d'accord : ce qui a été fait est en deçà des exigences du discours de la présidence de la Commission sur ce volet, mais également de tout ce que nous pouvons envisager en termes de régulation, notamment de droit de la concurrence. Il sera nécessaire de faire évoluer de nombreux droits avant de parvenir à intégrer dans le marché un acteur européen aussi fort que les Américains ou les Chinois.

S'agissant des écosystèmes, je ne sais pas encore ce que proposera la Commission. Elle a été interrogée sur l'organisation de la dimension écologique et économique des ressources autour des données, et sa réponse concernera donc également cette thématique. Le commissaire européen Thierry Breton a plusieurs fois évoqué ce sujet : les économies d'énergie réalisées dans d'autres secteurs pourraient être utilisées, mais il conviendra également de faire un bond technologique sur la consommation d'énergie : il s'agit donc là également d'une question de recherche, d'investissement et de régulation. Si nous voulons que la régulation ne soit pas fragmentée, elle devra être réalisée au niveau européen, notamment dans la stratégie des données. C'est également une course de vitesse pour les députés européens : tous les parlements européens réfléchissent aux sujets qui remontent des citoyens, des électeurs et des entreprises. Si le Parlement européen et la Commission ne vont pas assez vite, chacun fixera sa propre réglementation, et il sera très difficile de revenir dessus. Ceci explique que les textes sur le numérique et la souveraineté seront les premiers textes législatifs à sortir. Il s'agit de la priorité de la Commission. Je peux vous promettre un échange de bons procédés sur le travail parlementaire européen : nous ne travaillons pas assez en amont, ce qui nous met dans des situations complexes au moment de la ratification des décisions. Si un modèle européen se crée sur ces différents sujets (intelligence artificielle, données, savoirs, intégration des chaînes de valeur), il conviendra d'y réfléchir avec les parlements nationaux – et, notamment, avec vous. Nous devons créer, à l'Assemblée nationale, le cadre permettant ces échanges sur la régulation européenne.

Mme Danièle Hérin. S'agissant des modèles de données, la France est très performante sur le plan théorique. Le problème se pose plutôt au niveau industriel. Je crains que la tendance ne soit la même au niveau européen : les efforts se concentrent sur les modèles au détriment de la partie industrielle. Je ne doute pas que le travail mené sur les modèles soit fructueux, mais si l'industrie ne suit pas en Europe, ils pourraient être utilisés par les États-Unis et la Chine. Il me semble que la priorité est d'établir des partenariats entre les pays au niveau industriel. Serait-il envisageable que certains pays préparent une partie industrielle ?

M. Stéphane Séjourné, député européen. La perspective soulève des questions de droit de la concurrence. Ce droit, assez désuet, a toujours consisté à favoriser la concurrence pour offrir les plus bas prix au consommateur et accroître le pouvoir d'achat. La doctrine s'est avérée pertinente pendant un certain temps, permettant à de nombreuses entreprises de défendre une saine concurrence concernant leurs produits. Elle a également permis aux Européens de consommer moins cher. Le droit de la concurrence n'a pas non plus permis l'émergence de géants européens. Je crois que nous avons tiré les conséquences de ce qui a été manqué. Dans le cadre des politiques industrielles, la Commission européenne a soutenu le développement de projets importants et d'intérêt commun. Par exemple, les projets concernant l'hydrogène et la batterie du futur sont des projets intégrés. Au-delà de ces domaines, la Commission a identifié dans la filière de sécurité un certain nombre d'enjeux communs.

La prise de conscience de la problématique industrielle s'est opérée il y a cinq ans environ, lors du démantèlement d'entreprises qui devenaient trop grandes et trop concentrées. L'hydrogène est un enjeu d'application. La déclinaison du procédé peut être extrêmement importante dans l'industrie, mais elle suppose la capacité européenne à faire converger l'industrie vers cette énergie. Nous en sommes loin aujourd'hui. La démarche nécessitera de nombreux investissements durant les années qui viennent. L'Allemagne et la France sont les pays moteurs de ce projet. Le plan de relance européen doit défendre des investissements pour l'industrie du futur. En ce qui concerne l'hydrogène, de nombreux acteurs expliqueront sans doute que les procédés sont plus performants aux États-Unis ou en Chine. L'Europe ne devra donc pas céder face à des vents contraires probablement très forts. Elle doit résister si elle souhaite construire quelque chose de solide pour l'avenir. Ce projet pourrait également donner lieu à la création de nombreux emplois en Europe.

Mme Marion Lenne. Facebook a installé en 2015 son *hub* en intelligence artificielle à Paris. Ce lieu a sans doute été choisi pour l'excellence de la France en mathématiques. Aujourd'hui, ce sont cent chercheurs qui travaillent chez Facebook en recherche fondamentale et appliquée. Comment stimuler l'innovation pour s'orienter vers la souveraineté tout en conservant nos valeurs ? Par exemple, aujourd'hui, nous utilisons tous l'outil Zoom au lieu de Private Discussion, parce que cet outil ne permet pas le maintien d'une connexion visuelle lorsque les participants sont trop nombreux. Au-delà du droit, qu'il faut sans doute faire évoluer parce qu'il ne correspond plus à la réalité de la société, comment défendre l'innovation en France et en Europe ?

M. Stéphane Séjourné, député européen. Nous utilisons aujourd'hui Zoom parce que l'outil fonctionne bien et qu'il est très simple d'utilisation. Nous sommes aussi face à un enjeu d'ergonomie. Il nous faut construire un modèle européen fonctionnel, simple et économe. Le problème est le même concernant les téléphones portables sécurisés distribués aux ministres pour éviter la fuite de certaines données industrielles ou politiques sensibles. En définitive, personne ne se sert de ces téléphones, car leur utilisation n'est pas simple, et chacun utilise son portable personnel qui peut être piraté. La performance obtenue dépend bien entendu des moyens. Par exemple, l'État chinois a apporté une aide de 75 milliards de dollars à Huawei pour le développement de la 5G. La capacité d'investissement des États dans les grandes entreprises mondiales est déterminante. Outre les moyens, les outils doivent susciter la confiance du consommateur. L'enjeu clé au niveau européen est de rétablir la confiance. La transparence en est une condition, mais elle doit être un outil et non une fin. Une fois la transparence établie, les applications proposées doivent permettre aux entreprises européennes de répondre à un marché.

Le marché de la visioconférence est désormais très important en Europe, car tout le monde l'utilise. Le succès de Zoom repose sur sa simplicité et sa performance : l'outil nous permet d'organiser aujourd'hui une visioconférence dans de bonnes conditions. Nous ne disposons pas d'un outil de qualité équivalente en France ou en Europe. Je suis favorable à la conduite d'un travail sur ce sujet. Une étude de marché pourrait être conduite en vue de gérer la cybersécurité de ces plateformes.

M. Jean-Michel Mis, président. La notion de souveraineté numérique doit-elle s'entendre de manière collective en Europe ou chaque État manifeste-t-il des visions particulières et éventuellement contradictoires ? Lorsqu'on échange en France avec les start-up, au-delà des aides à l'innovation et à la structuration de filières, on pourrait aussi examiner les perspectives de commandes publiques. Une réflexion est-elle menée au niveau de l'Union européenne sur la commande publique en tant que moyen pour les entreprises de se développer à long terme ? La commande publique est assez largement pratiquée aux États-Unis, dans le cadre des activités « *business to government* ».

M. Stéphane Séjourné, député européen. Les Américains sont très forts dans le domaine du développement, mais ils sont en retard sur l'Europe en matière de recherche. Nous avons déposé de nombreux brevets sur les technologies d'avenir. Il s'agit de brevets essentiels et standardisés. Sur le marché de la 5G, il n'y a pas d'acteur américain. Nous disposons d'un certain nombre d'outils qui nous laissent penser que nous avons les moyens de développer une nouvelle industrie. Nous ne devrons non seulement poursuivre nos travaux de recherche fondamentale et de recherche et développement sur ces sujets, mais aussi accroître nos efforts dans les domaines d'application.

La commande publique est importante, à condition de cibler ce qui fonctionne. En d'autres termes, la commande publique doit aussi pouvoir orienter l'usage en fonction des besoins. Cette tendance est peu marquée en France, mais dans de nombreux pays d'Europe, la commande publique détermine l'usage d'un procédé ou d'une application. En ce sens, elle est un moteur de recherche et de développement des entreprises. L'Europe devrait être en mesure de demander un saut technologique et une innovation en fonction des besoins identifiés sur le terrain et de l'intérêt général. Les Scandinaves sont très forts dans ce domaine, les Français beaucoup moins. Nous regardons plutôt sur catalogue ce qui se fait et ce que nous pouvons utiliser. Il me semble que l'usage de la commande publique en France devrait évoluer de manière plus offensive. On pourrait concrètement demander au privé de se montrer inventif en établissant un cahier des charges. Pourriez-vous repréciser votre première question ?

M. Jean-Michel Mis, président. Elle portait sur la conception de la souveraineté numérique : diffère-t-elle selon les pays membres ou bien est-elle partagée ? Dans la même perspective, une liste commune de technologies de rupture a-t-elle été établie au niveau de l'Union européenne ou bien les priorités changent-elles d'un pays à l'autre ?

M. Stéphane Séjourné, député européen. La notion de souveraineté commence à faire consensus en raison du contexte politique international. En Europe, chacun perçoit désormais son intérêt à trouver les moyens d'agir et de réguler dans un marché de 500 millions de personnes, au demeurant assez modeste par rapport au marché chinois. Néanmoins, il existe des contradictions idéologiques entre les États membres. Certains conçoivent l'Europe comme une juxtaposition de marchés plutôt que comme une construction politique. Plusieurs États ont souhaité rejoindre l'Union européenne pour ce motif. Ils défendent leur capacité à être présents sur le marché unique européen sans vouloir dépasser ce stade.

Quant à la souveraineté politique, elle peut faire peur. En France, il semble assez largement admis que notre salut, notamment économique, repose sur l'entraide européenne, la

coopération et l'intégration d'un certain nombre de régulations. Tous les États ne partagent pas ces présupposés et il reste encore une bataille politique à mener sur le terme de souveraineté, même si l'utilisation de la notion a beaucoup progressé ces dernières années. Elle a notamment été portée dans le débat public européen par le Président de la République. Dans un discours récent, la présidente de la Commission européenne a employé à plusieurs reprises le terme de souveraineté. Elle n'aurait jamais pu l'utiliser il y a trois ou quatre ans au Parlement européen, car il n'était pas bien perçu. Aujourd'hui, si le sujet de la souveraineté ne fait toujours pas consensus, l'idée se précise qu'une souveraineté européenne est nécessaire afin que l'Union puisse agir par elle-même.

M. Éric Bothorel. Nous observons en France qu'il est très difficile de donner corps à la flotte dite « stratégique ». Nous sommes en particulier confrontés à un enjeu très important de câbles sous-marins qui dépasse notre seul territoire. La Russie a mené l'année dernière une simulation de coupage de tous les câbles qui n'étaient pas les siens. Nous voyons les grands acteurs du numérique devenir leurs propres opérateurs, alors que le marché était jusqu'à présent un marché de mutualisation. L'enjeu de la souveraineté se joue largement sous la mer. Des réflexions sont-elles conduites sur ce point comme sur la partie spatiale au niveau européen ? S'est-on interrogé sur la capacité de l'Europe à être souveraine dans le domaine des infrastructures sous-marines ?

M. Stéphane Séjourné, député européen. Ce n'est pas ma spécialité, mais à ma connaissance, l'Europe n'a pas à proprement parler de stratégie maritime dans les domaines que vous évoquez. En revanche, elle compte plusieurs champions européens, dont Orange, qui est un des seuls opérateurs à disposer d'un navire câblé. Les GAFAM ont conscience que les câbles sont un enjeu de souveraineté. Orange est en train de développer avec Google un câble transatlantique afin d'accroître les flux de données entre les États-Unis et l'Europe. L'objectif est de développer une véritable stratégie marine sur ces questions. Nous revenons ici à la question de la connectivité et de l'indépendance technologique. De manière générale, les mots d'ordre sont « oui à la connectivité », mais « attention à la dépendance technologique ». Nous devons rattraper notre retard dans un certain nombre de domaines, notamment la 5G. Si vous le souhaitez, vous pourrez obtenir davantage d'informations auprès de Pierre Karleskind et Dominique Riquet qui portent ces sujets au parlement européen.

M. Éric Bothorel. S'agissant de l'application « Tous anti-Covid », si elle n'est pas compatible avec l'application espagnole, cela posera problème. N'est-il pas regrettable que la France ait fait un choix de souveraineté en s'affranchissant de Google et d'Apple et que les autres États membres aient choisi d'autres architectures pour leurs applications?

M. Stéphane Séjourné, député européen. Le choix français a été dicté par l'enjeu de souveraineté des données, et pour les Français. Nous ne parlons pas ici de n'importe quelle donnée, mais des données personnelles et de santé qui sont particulièrement sensibles. La déception serait plutôt de ne pas avoir convaincu nos collègues européens et non de ne pas s'être laissé convaincre. Si l'Europe avait détenu une compétence sur le sujet, la situation aurait été différente. En l'occurrence, chaque État membre a souhaité défendre sa compétence sur le sujet. Le déploiement de ce type de dispositif n'est pas anodin pour l'opinion publique. Nous sommes tous très sensibles aux questions de liberté publique et de données personnelles. Quoi qu'il en soit, le confinement limite de façon drastique l'obligation de compatibilité entre un dispositif berlinois et un dispositif parisien. Les flux sont actuellement très limités entre la France et l'Allemagne. Le problème se posera plutôt lors du déconfinement. Si l'on avait disposé d'un système européen pendant les vacances d'été, alors que les déplacements étaient nombreux, la situation aurait pu être différente. Il convient donc de réfléchir à la compatibilité des applications entre un Français qui est à Barcelone et un Madrilène qui se rend à Barcelone.

Je n'ai pas de réponse précise à apporter sur ce point, mais je crois que le choix du système allemand n'aurait pas été la meilleure option.

M. Jean-Michel Mis, président. Avant les coopérations technologiques, ne pourrait-on commencer par viser l'interopérabilité entre les systèmes existants ? S'agissant des transports, elle permettrait par exemple de prendre un billet à la SNCF intégrant une correspondance en Allemagne et un vol. En ce qui concerne les orbites basses, où dominent SpaceX et Amazon, a-t-on engagé une réflexion sur le rôle de l'agence spatiale européenne ?

M. Stéphane Séjourné, député européen. Avant d'obtenir l'interopérabilité, il est nécessaire de mettre en place des standards communs. Toute la difficulté est là pour l'Europe. Par exemple, juste après Franco, les rails étaient plus étroits en Espagne qu'en France. Nous avons su entreprendre l'harmonisation des infrastructures ferroviaires en Europe. Nous devons maintenant progresser sur d'autres sujets. Les retards pris dans les infrastructures de nouvelle génération, notamment en 5G, sont un réel enjeu d'interopérabilité et de développement des systèmes. La situation n'est pas simple, étant donné que les grands acteurs verrouillent leur marché. Le standard commun pour l'interopérabilité signifie la concurrence pour de nombreux acteurs dans un certain nombre de domaines.

En ce qui concerne les relations entre la SNCF et la Deutsche Bahn, la coopération commerciale pourrait être renforcée. De manière générale, le régulateur ne peut pas tout faire. Les États membres et les entreprises doivent partager une volonté politique de converger. La situation ne peut évoluer si les entreprises n'affichent pas cette volonté. Nous sommes en train d'achever un trilogue sur le droit des passagers ferroviaires. Le travail effectué devrait contraindre les opérateurs à discuter entre eux et avec les entreprises commerciales. Le droit européen du passager entraîne des obligations à la fois pour les opérateurs et pour les entreprises qui gèrent les flux de passagers. L'interaction sera nécessaire entre ces deux groupes d'acteurs. Les bonnes pratiques pourront être partagées. J'ai pris l'exemple du domaine ferroviaire, mais l'on peut également penser à la route ou aux nouvelles technologies. La volonté politique est essentielle pour avancer dans le domaine des standards. La construction d'une législation européenne commune conduira les entreprises à dialoguer.

Audition, ouverte à la presse, de M. Charles Thibout, chercheur associé à l'Institut de relations internationales et stratégiques (IRIS) et chercheur au Centre européen de sociologie et de science politique (CNRS, EHESS, Paris 1)
(12 novembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. Philippe Latombe, rapporteur. Vous consacrez depuis plusieurs années au thème de la souveraineté et du numérique une réflexion ayant donné lieu à de nombreuses publications. Le thème de la souveraineté fait appel au cœur régalien des missions de l'État, mais nous engage également à une réflexion sur les armes économiques dont nous devons disposer pour défendre la place de notre pays et de l'Union européenne dans la compétition mondiale. Sur ces deux plans, régalien et économique, nous aimerions connaître votre opinion sur la montée en puissance de la notion de souveraineté numérique. Comment l'analysez-vous ? Que pensez-vous des positions adoptées au niveau national et au niveau européen par les autorités publiques ? Quelles appréciations portez-vous sur les initiatives législatives en cours ?

Cette problématique de la souveraineté et du numérique est riche de nombreux sujets, souvent porteurs d'enjeux majeurs pour la place de notre pays sur la scène internationale. Nous pouvons penser en premier lieu aux questions de cybersécurité et de cyberdéfense. La thématique de la souveraineté est ici incontournable puisqu'il s'agit de déterminer comment protéger les intérêts français de nouvelles menaces, immatérielles et déterritorialisées. Il s'agit également de définir de nouvelles modalités de discussion avec nos partenaires, européens et autres, pour engager des actions concertées, mais respectueuses de la souveraineté de chacun. Quelle est votre analyse de ces enjeux multilatéraux ? Comment percevez-vous le paysage international actuel ? Quelles devraient être selon vous les réponses françaises et européennes aux menaces de déstabilisation ou de désinformation en ligne ?

La souveraineté est aussi confrontée, sur un mode peut-être moins visiblement conflictuel, à la montée en puissance de nouveaux acteurs privés qui prétendent imposer leurs normes ou disposent d'un pouvoir de marché les rendant incontournables pour les consommateurs et les usagers. Comment la France et l'Union européenne peuvent-elles, selon vous, reprendre la main sur la définition des termes dans ces rapports nouveaux afin de ne pas en être réduites à une position strictement réactive voire passive ? Nous pourrons évoquer les multiples instances privées ou semi-privées dans lesquelles s'organise la gouvernance d'internet, l'attribution des noms de domaines par exemple, ainsi que les géants du numérique qui jouent un rôle de prescripteur de plus en plus important dans nos sociétés, qu'il s'agisse de nos modes de consommation ou de notre façon de nous informer. La crise que nous traversons avec la covid ne fait que renforcer ces tendances. Quelle réponse publique apporter au plan national, européen et international ?

Enfin, la défense de la souveraineté numérique passe aussi par celle d'une certaine autonomie matérielle et la défense de la promotion d'une industrie du numérique européenne compétitive et indépendante. Or, nous savons que l'Europe souffre de façon croissante du départ d'industries stratégiques pour le matériel informatique qui constitue pourtant le soubassement du développement du numérique. La dépendance aux solutions numériques extracommunautaires, aussi bien logicielles que matérielles, met-elle en cause selon vous l'autonomie européenne ? Comment contrer cette tendance ? Comment faire participer

l'innovation et à la recherche à une certaine forme de réindustrialisation dans les nouvelles technologies pour assurer une plus grande souveraineté européenne ?

M. Charles Thibout, chercheur associé à l'Institut de relations internationales et stratégiques (IRIS) et chercheur au Centre européen de sociologie et de science politique (CNRS, EHESS, Paris 1). Permettez-moi d'introduire mon propos par une citation : « *L'ensemble des produits américains doivent obtenir l'aval de la National Security Agency (NSA) pour être exportés. La NSA introduit systématiquement des portes dérobées ou* backdoors *dans les produits logiciels. Un système d'information et de communication (SIC) reposant majoritairement sur des produits américains comme Microsoft serait vulnérable car susceptible d'être victime d'une intrusion de la NSA dans sa totalité.* » Ceci, mesdames et messieurs les députés, n'est pas la citation d'un texte de propagande d'un État étranger, d'une agence hostile ou même d'une association militante de défense des droits des internautes. Il s'agit d'un extrait du rapport des experts militaires mandatés par le ministère de la défense en 2008 pour évaluer la valeur du projet de Microsoft alors présenté, à savoir un contrat de fournitures de logiciels Microsoft pour un peu plus de 180 000 postes de travail du ministère de la défense, contrat surnommé « *open bar* » qui, soit dit en passant, a été signé avec Microsoft Ireland. Ce contrat a depuis lors été renouvelé à deux reprises, en 2013 et en 2017.

Bien sûr, ce n'est pas le seul contrat entre l'État et les entreprises transnationales du numérique d'origine américaine, tant s'en faut. À vrai dire, nous ne comptons plus les contrats ou les partenariats noués entre l'éducation nationale, le ministère des armées, le ministère du travail d'une part et Microsoft, Cisco, IBM, Google, Amazon de l'autre. Le dernier exemple en date est le *Health Data Hub* (HDH) qui associe Microsoft et le ministère de la santé. Nous pouvons aussi évoquer Amazon par le biais d'Amazon Web Services (AWS) et son contrat avec la banque publique d'investissement BPI France.

Si, comme l'assurent les experts militaires en 2008, lier contrat avec ces entreprises aboutit inévitablement à, je les cite, « *la perte de la souveraineté nationale* », comment expliquer que ces avertissements, qui n'ont cessé de croître au fil des années avec les révélations d'Edward Snowden et de WikiLeaks, n'ont jamais été entendus ?

Certains de ces experts ont affirmé, de façon anonyme bien sûr et je leur laisse l'entière responsabilité de leurs propos, que la réponse était à chercher du côté de la corruption de certains décideurs de l'époque. Il ne faut pas écarter cette hypothèse, mais elle me semble trop partielle pour comprendre notre situation.

Ce que nous vivons est l'aboutissement logique, contingent, mais logique, d'une myriade de décisions, de hasards, d'aléas politiques et géopolitiques qui tirent leur origine du virage idéologique que l'Europe a pris voici quarante-cinq ans, ce que d'aucuns ont appelé le tournant néolibéral.

Je sais ce que, hors du champ scientifique, ce terme peut avoir de scandaleux, ou du moins de controversé, mais je ne suis pas là pour faire de la politique, ni même pour prendre position. Je suis là seulement pour vous dire ce qui, de mon point de vue de chercheur en sciences politiques et en sciences sociales, permet d'expliquer la situation dans laquelle se trouvent actuellement l'Europe et la France et esquisser quelques pistes de réflexion.

L'Europe est néolibérale depuis les années 1970-80. En France, l'historien Gilles Richard a fait remonter le néolibéralisme à l'élection de Valéry Giscard d'Estaing. Au-delà de la querelle politique et philosophico-sémantique autour de ce terme, il importe de comprendre qu'un État néolibéral, dans la hiérarchie des objectifs de politique publique, fait toujours primer sur l'intérêt national l'intérêt économique, quel qu'il soit et d'où qu'il vienne j'insiste

sur ce point. Pour le dire autrement, en reprenant les mots de Gilles Deleuze dont nous commémorons cette année le vingt-cinquième anniversaire de la disparition, « *l'État totalitaire* – c'est la manière dont il conceptualise l'État néolibéral – *est entièrement tourné vers le développement du marché extérieur et, à l'inverse, il délaisse voire il tend à détruire le marché intérieur* ».

Le néolibéralisme qui s'est progressivement érigé en idéologie nationale, en doctrine d'État, a au fil des décennies privilégié le développement économique là où la dynamique économique se trouvait, là où pouvaient émerger de nouveaux marchés, de nouveaux projets d'investissements. Ceci explique en partie la prédominance du terme « compétitivité » dans le champ lexical de nos dirigeants nationaux et européens. Nous savons aujourd'hui que deux pays en ont grandement bénéficié : les États-Unis et la Chine.

Quant à l'Europe, elle a, pour simplifier le trait, fait un pari : celui d'une libéralisation des flux économiques, financiers et commerciaux. Cette circulation des capitaux devait, bon an mal an, par sa généralisation, rencontrer les intérêts de toutes les parties prenantes de sorte qu'un système mondialisé d'interdépendance généralisée devait *ipso facto* en surgir et pérenniser la pacification des relations internationales, en un mot en finir avec la guerre.

Le problème, vous le savez sans doute, est que ce pari a été perdu, pas sur la guerre – Dieu nous en préserve ! –, mais nous sommes entrés dans un jeu dont nous ne maîtrisons pas les règles. Plutôt, nous nous sommes appliqué des règles que d'autres ont nonchalamment écartées. Nos totems – le libre-échange, la concurrence libre et non faussée, l'hygiène budgétaire… – nous ont placés dans une position de faiblesse à l'égard des États-Unis et de la Chine qui ne se sont pas encombrés de telles restrictions juridico-économiques, partiellement infondées au demeurant, notamment la règle des 3 % de déficit.

Je fais ce détour pour insister sur un point qui me paraît essentiel : la question de la souveraineté numérique est à la fois un enjeu et un objectif éminemment politiques. Bien avant de nous demander quel chemin technologique nous devrions emprunter pour atteindre cet objectif, il faut dessiner le chemin politique. Cela me paraît capital d'autant plus que cette réflexion brille par son absence dans le discours des responsables politiques européens.

Qu'entendons-nous par souveraineté numérique ? C'est le pouvoir suprême du souverain, qu'il s'agisse de l'État, de la Nation ou même de l'individu, à maîtriser ses données et les instruments de collecte, de stockage, de traitement, de circulation de ces données à travers les trois couches du cyberespace.

Ces trois couches sont :

– la couche matérielle : tous les périphériques d'accès et les infrastructures nécessaires au fonctionnement chez les fournisseurs de connexion, les serveurs, les câbles sous-marins, les routeurs… et leurs différents éléments tels que les microprocesseurs, les matériaux stratégiques comme le lithium, le cobalt, l'indium, le platine, voire les sources énergétiques ;

– la couche logicielle ou logique : les protocoles qui permettent aux machines de communiquer entre elles et d'échanger des données, les applications et les standards qui en conditionnent l'utilisation ;

– la couche sémantique qui se rapporte proprement au contenu informationnel de l'internet : l'ensemble des messages qui passent par internet, les interactions sociales, les échanges d'informations…

Deux pays seulement sont parvenus à un tel niveau de souveraineté : les États-Unis et la Chine. Sans faire le détail de l'histoire de l'innovation de ces deux pays, j'insiste sur quelques grandes tendances de ces deux systèmes technopolitiques qui peuvent nous inspirer, au-delà de la capacité de contrôle de ces deux États sur les trois couches.

Le plus important à mon sens est que ces deux États ne sont pas libéraux au sens où nous l'entendons habituellement. C'est évident pour la Chine. Pour les États-Unis, il faut avoir en tête que l'ensemble de l'architectonique technoscientifique est consubstantiellement lié à la domination de l'État fédéral sur son appareil productif et d'innovation, depuis la Seconde Guerre mondiale et encore de nos jours. Cette économie est communément qualifiée d'économie en réseau. Je m'inscris en faux car ce concept accorde à mon avis aux acteurs économiques et universitaires un rôle surestimé.

Il n'est pas possible en effet de comprendre le développement spectaculaire des géants du web, les GAFAM, sans le concours principiel de l'administration centrale dans la régulation du marché des brevets par exemple ou dans les partenariats entre universités, start-up et grandes entreprises sous l'égide d'agences fédérales, de la *Defence Advanced Research Projects Agency* (DARPA) notamment, ainsi que dans l'externalisation réussie de l'innovation par les grandes sociétés par le rachat de brevets et de start-up ou dans l'obtention de marchés à l'étranger et la protection du marché national. Il faut compter de plus les subventions, les exonérations fiscales, les contrats très lucratifs qui continuent de les abreuver en capitaux. Je rappelle que, l'an passé, Amazon n'a payé aucun impôt des sociétés aux États-Unis alors que les relations entre Donald Trump et Jeff Bezos sont exécrables. Microsoft a remporté l'an passé un contrat de 10 milliards de dollars pour le *cloud* du Pentagone.

Concrètement, IBM ne serait pas devenu la première entreprise d'informatique du XX^{e} siècle sans le *New Deal* de Franklin Roosevelt. Facebook n'aurait peut-être pas vu le jour sans le possible soutien financier d'une tutelle, la société de capital-risque de la *Central Intelligence Agency* (CIA). L'ascension fulgurante de Google n'aurait sans doute pas été telle sans l'aide financière apportée aux travaux de deux jeunes doctorants de l'université Stanford par la *National Science Foundation* (NSF) avec d'autres agences fédérales de premier ordre.

Je ne dis pas qu'il faut dédaigner le rôle des inventeurs talentueux et des programmes de recherche innovants, mais nous pouvons douter de la réussite de ces entreprises si elles n'avaient pas été soutenues, orientées dans leurs décisions par l'État. J'irai même plus loin en disant que ces entreprises n'auraient pas connu un tel destin si elles n'avaient pas évolué dans ce que nous pouvons appeler une économie administrée, un régime dirigiste.

Quant à la Chine, nous voyons qu'il est incohérent d'y voir un modèle antinomique de celui des États-Unis. Plus encore, la Chine a conçu depuis le début des années 1980 son modèle de développement technologique sur le modèle américain. Il faut dire qu'elle partait de loin. La révolution culturelle qui fut déjà un phénomène terrible s'est doublée d'une purge incommensurable du monde de la recherche universitaire avec la perte d'au moins un million d'étudiants de premier cycle et de 100 000 étudiants de second cycle, ce qui explique encore aujourd'hui ce manque de talents.

Contrairement aux États-Unis, la Chine n'avait ni capital économique et technique, ni serveur racine, ni câble sous-marin, ni géant technologique à sa disposition pour asseoir sa souveraineté. Qu'a-t-elle fait ? Elle a importé ces technologies en faisant miroiter aux entreprises les débouchés mirobolants que laissait espérer son immense marché, pas que dans le numérique d'ailleurs. Entre aspiration à la modernisation et hantise de l'occidentalisation, la Chine a compris l'importance cardinale de maîtriser les couches techniques du cyberespace – couche matérielle et couche logicielle – et de contrôler ce faisant les données.

La prépondérance américaine est réelle dans ce domaine : 38 % des centres de données de la planète se trouvent actuellement aux États-Unis et les communications numériques entre l'Europe et l'Asie passent à 97 % par les États-Unis. La Chine a donc compris l'importance de rapatrier ces données en Chine, sur son territoire et de faire en sorte que les acteurs qui collectent les données en Chine, y compris les acteurs étrangers, les stockent et les traitent sur le territoire national chinois. C'est tout l'enjeu de la loi sur la cybersécurité du 1er juin 2017. Il en allait de sa souveraineté et la souveraineté constitue la quintessence de son programme politique que nous pouvons résumer par le triptyque « Prospérité, stabilité, puissance ».

Nous avons donc avec la Chine l'exemple d'un pays qui a décidé de devenir souverain sur l'ensemble des trois couches du cyberespace et s'en est donné les moyens. Sur la couche matérielle a été mis en place un système de contrôle des entrées-sorties des données, appelé le « Grand Firewall » de Chine ou « Bouclier doré ». Il permet à l'État de maîtriser avec un degré d'efficacité relativement important ce qui entre et sort du cyberespace chinois.

Sur la couche logique, la Chine est parvenue à dupliquer l'offre américaine de services en produisant une offre nationale avec l'émergence et le développement d'acteurs homologues : Baido, Alibaba, Tencent, Huawei… qui, peu ou prou, remplissent les missions et offrent les mêmes types de services que Google, Amazon, Facebook, Apple… Ces entreprises sont très proches de l'État-parti. Elles sont juridiquement soumises à un devoir d'étroite coopération avec les pouvoirs publics chinois en vertu de la loi sur l'espionnage de juin 2017 et de la loi sur le contre-espionnage de 2014 qui imposent à tout citoyen chinois et à toute organisation de droit chinois de partager les informations qu'ils ont en leur possession avec les services compétents, au premier chef desquels les services de renseignement.

Enfin, la Chine s'est dotée d'un ensemble de structures de contrôle, en clair de censure, qui agissent directement sur la couche sémantique du cyberespace et sont censées juguler la diffusion de messages et de commentaires critiques à l'égard du régime et plus largement du système sociopolitique chinois.

En définitive, la Chine s'est donné les moyens d'être souveraine sur le cyberespace, suivant bien sûr sa propre critériologie totalitaire qui se manifeste particulièrement sur son contrôle resserré de la couche sémantique et par le développement d'un système d'étroite coopération entre l'État-parti, la recherche publique et les firmes technologiques. C'est un système que j'ai appelé dans certains de mes travaux un complexe techno-partidaire.

À propos de la Chine, il faut également avoir en tête que, alors qu'elle était dans un état de totale subordination vis-à-vis des États-Unis, elle est parvenue à asseoir sa souveraineté numérique. Rappelons-nous que, jusqu'en 2004, la Chine avait un produit intérieur brut (PIB) inférieur à celui de la France. Son PIB par habitant est encore aujourd'hui quatre fois plus faible que celui de la France. Il n'y a donc pas de fatalité.

Si nous nous en tenons à la lettre de l'intitulé de la mission d'information, ces deux pays peuvent-ils inspirer la France et l'Europe ? Si nous tenons pour acquise cette ambition politique de faire advenir une souveraineté numérique française et/ou européenne, je pense que oui, d'abord en ramenant la puissance à un rôle de coordonnateur, d'architecte, de cause motrice et intellectuelle des grandes orientations de la recherche, de la politique industrielle, d'un point de vue tant financier que décisionnel. Il s'agit d'un rôle d'État stratège en somme, capable de puiser dans le bassin scientifique et technique national ou continental les bonnes personnes pour penser stratégiquement et mettre en application des décisions démocratiquement légitimées.

Bien entendu, il serait vain de reproduire tels quels les modèles américain et chinois où le consentement de la population est soit une variable d'ajustement soit une lubie occidentale. En revanche, nous pouvons nous inspirer de leur gestion de l'innovation, notamment des États-Unis avec la DARPA. Une initiative européenne s'est justement mise en place dans cette optique, la *Joint European Disruptive Initiative* (JEDI) à laquelle je participe. C'est une fondation autonome qui a le mérite d'un point de vue tactique et technique de montrer la pertinence d'un changement de modèle dans la conception des innovations de rupture. Elle inscrit la recherche dans le secteur des technologies émergentes non comme une fin en soi, ce qui n'aurait aucun sens, mais comme un moyen mis au service de causes supérieures dans le domaine de l'environnement et de la santé par exemple.

La France et l'Europe ont donc tout à fait les moyens de bâtir leur souveraineté numérique, théoriquement du moins. Toutefois, la question *princeps* n'est pas technologique. Les moyens techniques et tactiques sont en notre possession, fut-ce virtuellement. La question est à mon avis bien davantage d'ordre politique et géopolitique. Il s'agit de convenir d'intérêts et d'objectifs communs, d'en déduire un ordre de priorité, les stratégies adéquates et bien entendu d'anticiper, de se projeter vers l'avenir que nous souhaitons précisément voir advenir.

Il s'agit également de rompre avec des ratiocinations juridiques et le culte de la régulation, de promouvoir la commande publique qui est fondamentale comme nous l'avons vu dans les exemples américains et chinois. Il faut restaurer les conditions de possibilité d'une recherche libre et sereine et, bien sûr, emporter l'adhésion de la population.

Si tout cela avait existé, la braderie de la branche énergie d'Alstom à General Electric n'aurait pas eu lieu. Alcatel n'aurait pas été vendu à Nokia et Nokia ne serait pas aujourd'hui en train de marginaliser la France dans sa stratégie de développement. En remontant encore plus loin, Louis Pouzin, l'un des pères de l'internet, un Français, aurait été suivi par l'État et l'histoire aurait sans doute été tout autre. D'ailleurs, nous ne serions pas là pour en parler.

En l'état actuel, il me semble tout à fait impossible d'envisager une Union européenne technologiquement puissante et souveraine si nous nous en tenons aux coordonnées économiques et géopolitiques qui guident l'Europe depuis le traité de Rome et se sont calcifiées au fil des décennies. Il faudrait d'abord un souverain européen ce qui est pour l'heure introuvable. À défaut, il faudrait une communauté d'intérêts suffisamment autonome pour résister aux tropismes atlantiste, slave ou extrême-oriental. Cette communauté d'intérêts n'existe pas encore. Cela n'exclut pas des coopérations ponctuelles entre quelques pays lorsque les intérêts de chacun se rejoignent, mais, s'il s'agit de conjoindre souveraineté numérique européenne et française, je crains que cela ne revienne à chercher la quadrature du cercle.

N'oublions pas que, si nos trois derniers Présidents de la République, Jacques Chirac, Nicolas Sarkozy et François Hollande, ont été espionnés par la NSA, c'est par l'intercession et avec le concours actif du *Bundesnachrichtendienst* (BND), le service fédéral de renseignement allemand, équivalent de notre direction générale de la sécurité extérieure (DGSE).

M. Philippe Latombe, rapporteur. Vous avez dit qu'il faut que l'État soit un véritable État stratège et qu'une ambition politique soit présente. Par ailleurs, vous avez suggéré de copier la DARPA dans le champ européen et parlé de la fondation JEDI. Est-ce ce mode de fonctionnement par une fondation autonome qui doit intervenir ? Cela doit-il être une agence plus structurée, qui dépende directement d'organismes européens ? Comment sentiriez-vous personnellement la création et la gouvernance de l'équivalent de la DARPA ?

Cela permettrait peut-être de répondre à votre autre question sur l'absence de souverain et au manque d'une communauté d'intérêts stable.

M. Charles Thibout. Je pense que la vocation de JEDI est de devenir une agence européenne. Cette ambition de souveraineté numérique, technologique est apparue voici trois ans environ et est montée en puissance. Il est étonnant que les décideurs européens ne se soient pas emparés de cette initiative privée pour l'intégrer dans les institutions européennes. Bien sûr, reproduire un schéma bureaucratique et technocratique comme il en existe trop souvent dans l'Union européenne n'a pas d'intérêt, mais garder cette souplesse inspirée du modèle de la DARPA me paraîtrait une bonne chose. Il faut rappeler que la DARPA n'est pas du tout une agence de recherche, mais une agence qui finance et coordonne la recherche. Elle a mené à des succès méritoires, à internet et auparavant à l'*Advanced Research Projects Agency Network* (ARPAnet) qui est le fruit d'une mise en commun de chercheurs d'université. La DARPA est aussi à l'origine du *Global Positioning System* (GPS), des drones.

Ce n'est pas suffisant, mais c'est un outil intéressant dont les responsables politiques français et européens auraient tout intérêt à s'emparer pour devenir une pierre de touche de notre capacité à nous tourner vers l'innovation.

M. Philippe Latombe, rapporteur. Vous avez évoqué le fait que l'Europe s'est construite sur des principes que les autres pays, notamment les États-Unis et la Chine, avaient abandonnés : la concurrence libre et non faussée, le fait que les consommateurs soient éclairés et libres de choisir les produits. Vous avez ensuite parlé de la façon dont les économies américaines et chinoises sont administrées, l'une par l'État, l'autre par le parti-État. Vous avez dit que l'Europe souffre d'être coincée entre ses valeurs de concurrence libre et éclairée ce qui fait que les marchés publics ne sont pas dirigés comme ils devraient l'être.

Faudrait-il, selon vous, que nous changions complètement le fonctionnement de nos marchés ? Si nous n'y arrivons pas parce que des pays s'y refusent pour des raisons idéologiques, faut-il que nous ayons des règles différenciées au sein de l'Union européenne ? Comment permettre que les marchés publics soient une source de financement de la souveraineté comme c'est le cas aux États-Unis ?

M. Charles Thibout. Vous avez raison. Les traités européens empêchent aujourd'hui un État de favoriser une entreprise nationale, voire de favoriser une entreprise communautaire au détriment d'une entreprise extra-européenne, ce qui est un peu problématique pour favoriser la souveraineté numérique. Nous nous cantonnons donc à des mesures réactives et défensives du type concurrence libre et non faussée. C'est probablement ce qui se produira encore avec le *Digital Services Act* et le *Digital Market Act*.

Je pense que la question est aujourd'hui celle des traités, de l'aspect juridique qui constitue l'Union européenne. Il faut sans doute dépasser ce modèle. À vingt-sept, trouver un accord qui reposerait sur des intérêts et des objectifs communs et donc sur une ambition politique commune me paraît tout à fait irréalisable. Nous imaginons mal que l'Irlande, par exemple, prenne des décisions contraignantes contre des entreprises dont le siège social européen se situe en Irlande. Le Premier ministre du Luxembourg a indiqué récemment que son pays soutenait Google et il est étonnant qu'un pays se place ainsi, aussi manifestement, derrière une entreprise.

La concurrence libre et non faussée est à mon avis un pis-aller qui ne résout rien en réalité. Même si vous démantelez les GAFAM, si vous faites en sorte que les règles soient les mêmes pour tous, cela ne fera pas surgir des géants européens. L'innovation ne se décrète pas, elle a besoin de fonds et du soutien de l'État, d'un État stratège. Pour le moment, l'Europe

n'est pas en position d'offrir cette figure de l'État stratège que requerrait cette souveraineté numérique.

M. Philippe Latombe, rapporteur. Si nous n'arrivons pas à trouver à vingt-sept cette modification des traités, faut-il que nous ayons une géométrie européenne un peu différente ? Nous pouvons peut-être régler le problème de l'Irlande avec la question fiscale, mais c'est plus compliqué avec le Luxembourg. Nous avons aussi des pays de l'est de l'Europe qui ont une vision différente. Comment faire pour que les marchés publics aillent vraiment vers le territoire ?

M. Charles Thibout. Je crois qu'il faut modifier les traités.

M. Philippe Latombe, rapporteur. Quitte à en perdre sur le bord de la route ?

M. Charles Thibout. Oui, bien sûr.

Mme Virginie Duby-Muller. Un de nos handicaps au niveau européen n'est-il pas le fait de ne pas avoir d'acteurs transnationaux puissants tels que les GAFAM et les entreprises du web chinois (BATX) ? Nous avons bien compris que nous avons des atouts technologiques, mais qu'il nous manque la volonté et la cohérence politique. Que faire en termes de méthodes pour avancer concrètement sur cette question de la souveraineté numérique ? Je crois qu'il y a aujourd'hui une véritable urgence.

M. Charles Thibout. Pour parer au plus urgent, je ne sais pas ce que pourrait faire l'Europe, mais je sais que la France dispose d'ores et déjà d'outils. Je pense notamment à la mention « Spécial France ». Cette mention peut être apposée par exemple sur un contrat. Je vous renvoie à l'article 65 de l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. Cette mention a ceci d'intéressant qu'elle permet de restreindre à de ressortissants français l'accès à des informations ou à des supports, classifiés ou non. En l'occurrence, il s'agirait de l'accès à des données.

Je cite l'article : « *Des informations qui ne sauraient, en aucune circonstance, être communiquées en tout ou partie à un État étranger ou à l'un de ses ressortissants, à une organisation internationale ni à une entreprise de droit étranger, même s'il existe avec cet État ou cette organisation un accord de sécurité.* »

La mention « Spécial France » est donc un outil simple que nous pourrions utiliser tout de suite. Elle ne coûterait pas un euro au contribuable et est susceptible de parer au plus urgent. Je ne suis ni un spécialiste ni un technicien, mais je pense qu'elle pourrait par exemple être appliquée dans le cas du *Health Data Hub*.

La question des acteurs transnationaux est bien sûr une faiblesse d'une certaine manière, mais il ne faut pas non plus idéaliser ce modèle. Il fonctionne effectivement très bien pour la Chine, mais parce que c'est un État totalitaire qui fait en sorte que ces entreprises soient consubstantiellement liées à l'État-parti. Des cellules du Parti communiste sont présentes dans les comités de direction. Ces entreprises ont des liens historiques très fort avec l'État central. Il existe tout un jeu de coopération pour étendre leurs activités le long des nouvelles routes de la soie.

Côté américain, c'est plus ambigu. Une sorte de dissociation d'intérêts s'opère actuellement entre certaines de ces grandes entreprises et l'État fédéral, notamment en raison de l'émergence de la Chine et du pouvoir économique que constitue la Chine. C'est un marché

extrêmement attractif qui pousse certaines de ces entreprises à vouloir nouer des liens de coopération avec l'État sur des technologies tout à fait critiques comme l'intelligence artificielle, y compris des liens de coopération avec des institutions militaires de l'État chinois. Cela a poussé par exemple Patrick Shanahan, à l'époque secrétaire ou secrétaire adjoint à la défense, et le chef d'état-major des armées à parler dans une audition de traîtrise de Google. Si nous pensons en termes d'intérêt public et que, par définition, l'intérêt public est représenté par l'État, nous pourrions rencontrer cet obstacle.

M. Philippe Latombe, rapporteur. Vous avez évoqué les relations entre les géants et leur pays d'origine. Nous avons vu le patron d'Alibaba avoir quelques petits soucis voici quelques jours avec l'introduction en bourse de l'une de ses filiales. Cela ressemblait à une forme de sanction. Ce système pose-t-il des problèmes aux États-Unis et à la Chine et réfléchissent-ils déjà à l'étape suivante ? Quelle serait cette étape, pour que nous ne fassions pas la même bêtise et ne construisions pas des géants qui nous poseraient plus tard des problèmes ? Ne pourrions-nous pas avoir une réflexion prospective sur ce sujet ? Comment voyez-vous l'avenir de ces géants ? Seront-ils démantelés ou non ?

M. Charles Thibout. Je ne pense pas que le fait qu'ils soient démantelés ou non change grand-chose, en tout cas pour nous. Les deux grands exemples du XX^{e} siècle sont la Standard Oil au début du siècle et AT&T au début des années 1980. Leur démantèlement a provoqué de nouvelles ententes qui ont substitué un oligopole à un monopole. Je crois que démanteler n'a pas grand intérêt.

Les relations entre les États et ces entreprises m'intéressent beaucoup. Je pense que cette réflexion n'existe pas aux États-Unis dans la mesure où la frontière entre public et privé, entre État et entreprise est de plus en plus floue. Il se produit une sorte d'hybridation ; des personnalités très importantes de ces entreprises accèdent à des postes de conseil et même de décision au sein l'appareil d'État comme Eric Schmidt, l'ancien président-directeur général (PDG) de Google qui a été nommé en 2016 à la tête d'un organe consultatif important du Pentagone. Il est chargé de faire le lien entre la Silicon Valley et le département de la défense. Il est pressenti pour diriger un groupe de travail sur les industries de nouvelles technologies au sein de la Maison-Blanche sous l'administration Biden. L'équipe de transition de Biden comprend notamment l'ancienne directrice juridique adjointe de Facebook, l'ancienne vice-présidente aux affaires gouvernementales d'Apple. Des liens existent donc avec des phénomènes de « pantouflage » – *revolving doors* – entre l'État fédéral américain et ces entreprises de sorte qu'émerge une figure hybride de l'État. Ces phénomènes ont toujours existé, de tout temps et partout, mais ils sont actuellement assez concentrés dans le secteur des nouvelles technologies numériques.

En Chine, nous avons effectivement vu une petite sanction de la part de l'État chinois sur Alibaba et Jack Ma mais, pour le moment, le modèle fonctionne et demeurera encore pendant plusieurs années. En 2018, Jack Ma alors PDG d'Alibaba, Pony Ma de Tencent et Robin Li de Baidu ont été nommés vice-présidents d'une commission de sécurité de l'internet chinois. Il leur a été délégué un pouvoir régalien de contrôle et de sécurité de l'internet, ce qui prouve que ces entreprises bénéficient d'une véritable confiance de l'État. Je ne crois pas que ce soit sur le point de changer.

M. Denis Masséglia. Je souhaite faire part de mon inquiétude quant à la nécessité d'avoir un marché suffisamment important en termes de consommateurs pour développer une souveraineté numérique. La Chine et les États-Unis sont des marchés de plusieurs centaines de millions de consommateurs ce qui n'est pas le cas de la France seule. Notre marché étant petit et nos financements relativement limités, je m'interroge sur la capacité qu'a la France de faire front seule et de faire face à la mise en place d'une souveraineté numérique.

Par exemple, le plan qu'a porté Cédric Villani sur l'intelligence artificielle prévoit un investissement de 1,5 milliard d'euros sur cinq ans tandis que la Chine, en 2017, investissait plus de 7 milliards d'euros. Cela représentait presque la moitié des financements mondiaux *via* des start-up pour l'intelligence artificielle : près de la moitié pour la Chine, 38 % pour les États-Unis. Vous voyez ce qu'il reste pour les autres pays du monde…

Pour moi, malgré la volonté du Gouvernement, la solution ne peut pas passer par une stratégie uniquement française. Elle doit être définie à l'échelle de l'Union européenne. Je crois qu'il serait nécessaire que nous ayons un ministère propre, référent, indépendant qui puisse concevoir des stratégies au niveau de l'Europe de façon à mettre en place une véritable stratégie avec de vrais financements. Pour réussir, il faut des financements conséquents et un marché unique qui puisse offrir des possibilités aux entreprises qui investissent dans ce domaine.

Il faut une Europe forte, unie, puissante, capable de mettre de côté les quelques points sur lesquels nous n'arrivons pas à nous mettre d'accord. La solution est que nous travaillions collectivement pour le bénéfice de tous.

M. Charles Thibout. Votre réflexion est intéressante. Comme vous l'avez rappelé, le problème est l'extrême difficulté à trouver un socle d'intérêts communs suffisamment fort et puissant pour développer une vision stratégique bien « cortiquée » et mettre les financements nécessaires sur la table.

La France est peut-être un acteur trop faible et trop petit pour pouvoir se hisser à la hauteur des États-Unis et de la Chine. Pourtant, l'histoire tend à nous montrer que ce n'est pas si clair. À la fin de la Seconde Guerre mondiale, la France était dans un état déplorable de destruction. Les Américains ont aidé *via* le plan Marshall car leurs intérêts étaient en jeu, mais il faut se souvenir de ces couvertures de magazines américains des années 1960 où la France faisait peur. Les États-Unis pensaient que la France était le prochain leader géopolitique mondial du fait justement de son rattrapage forcené durant les Trente Glorieuses. C'est à mon avis dû à deux phénomènes : au rattrapage économique, avec énormément d'interventions publiques, financières et décisionnelles, et à un plan.

Cela revient à l'esprit de nos dirigeants actuels avec le Haut-Commissariat au Plan en cours de construction. Même s'il paraît archaïque, le plan a ceci d'intéressant de se projeter sur le temps long, à dix, vingt ou trente ans, donc au-delà des aléas électoraux, des changements de majorité qui, bon an mal an, font ce qu'elles peuvent, mais ont tout de même tendance à aller à l'encontre des décisions précédentes. Un plan ou un équivalent donnerait la possibilité de projeter des financements sur le long terme dans des objectifs ou des initiatives identifiés, objectifs que nous mettrions à jour régulièrement bien sûr. Il me semble que ce serait une étape intéressante d'autant plus que la France, en termes de financement, a l'avantage qu'une grosse partie de sa dette est encore actuellement possédée par les citoyens français. La dette française n'est donc pas un poids, mais un actif qui peut être délibérément mis au profit d'une politique de grands travaux en quelque sorte.

M. Denis Masséglia. Votre analyse est extrêmement intéressante et je souhaite réagir. La France a effectivement investi massivement à la sortie de la Seconde Guerre mondiale sur certaines technologies, mais nous avons ciblé deux ou trois technologies, par exemple le nucléaire. Nous avons décidé de développer la bombe nucléaire et l'énergie nucléaire. Ce sont donc des sujets très complexes, mais très ciblés. Nous savions où aller, avec une stratégie d'investissements canalisée vers cet objectif.

Dans le cas du numérique, nous ne savons pas réellement où nous devons aller. Si vous saviez ce qui marchera dans cinq ou dix ans, vous ne me le diriez pas parce que vous investiriez massivement dessus. Il existe de nombreuses possibilités, beaucoup de fléchages d'argent à faire. Il faut donc à mon avis mettre, au prorata du PIB, beaucoup plus d'argent sur la table que ce n'était le cas à la sortie de la Seconde Guerre mondiale.

Par ailleurs se pose le problème de la volonté des concitoyens à construire quelque chose. Ma femme s'étonnait de voir de nombreuses personnes avoir des T-shirts siglés « NASA » en France. Je lui ai répondu que ce serait bien que nous fassions de même avec des T-shirts siglés « ESA ». Elle m'a regardé et demandé : que signifie « ESA » ? L'*European Space Agency* (ESA) est tout de même quasiment l'équivalent de la *National Aeronautics and Space Administration* (NASA), mais la capacité que nous avons de créer des choses magnifiques ne fait plus rêver les Européens.

Quand donnerons-nous envie à nos ingénieurs d'aller marcher sur la Lune ? Quand donnerons-nous à nos ingénieurs l'envie de créer le *smartphone* de demain ? Notre ambition n'existe plus alors que les ambitions américaines et chinoises existent. Nos politiques ne font plus rêver les chercheurs ; c'est dommage. Le peuple français, le peuple européen ne rêvent plus à ce qu'ils sont capables de construire. Nous n'avons plus de projet qui donne à nos concitoyens l'envie de s'investir.

M. Charles Thibout. Je vous rejoins sur le fait que nous ne rêvons pas de projet scientifique et technique, du moins que cela n'apparaît pas, ce qui tranche effectivement avec les États-Unis et la Chine. Dès le début du XX^{e} siècle, les chroniqueurs relèvent dans la population américaine une véritable appétence pour la science et le progrès technique.

En Chine, il a longtemps existé un dilemme entre une volonté farouche de modernisation qui passait en grande partie par une modernisation technique et technologie et la hantise que cette modernisation entraîne une occidentalisation, une importation des cultures et des institutions occidentales.

Nous ne pouvons pas mettre de côté l'importante méfiance des populations européennes envers leurs dirigeants qui se manifeste par des mouvements populaires à tendance insurrectionnelle, par la montée de l'extrême-droite et parfois son accession au pouvoir. Cette extrême-droite semble elle-même légitimée par les institutions européennes qui posent un voile pudique sur les agissements de tel ou tel dans certains pays envers les migrants ou le droit des femmes.

C'est à la fois la tragédie et le grand mérite de nos institutions. Nous sommes habillés pour un Général qui avait tout d'un monarque républicain capable de donner un horizon par un discours et un programme politiques. L'horizon est aujourd'hui assez introuvable. Nous avons du mal à nous projeter vers l'avant du fait des contraintes économiques, des contraintes institutionnelles européennes, d'où l'intérêt de poser une ambition au niveau français et/ou européen. Il faut inclure la population dans cette ambition, faire en sorte que la population veuille d'un développement technique dans telle technologie en particulier, parce que ce développement la fait rêver ou qu'il créera de l'emploi ou qu'il fera monter le pouvoir d'achat ou que les conditions de vie s'amélioreront… Cela signifie recréer un marché intérieur, relancer la consommation.

Sur la question des technologies, il est exact que nous avons tendance ces dernières années à jouer à passer d'une technologie à une autre, sans même savoir vraiment quelle est la différence. Cet ensemble crée un répertoire technologique assez confus et dense. Les responsables politiques peuvent consulter massivement les spécialistes de ces domaines et

savoir ce que ces spécialistes voient comme ouvertures techniques et technologiques apportées par ces différentes découvertes scientifiques. Par exemple, rien n'assure que le quantique amènera vraiment à cet ordinateur quantique dont nous rêvons. À partir de cette connaissance scientifique, nous pourrons dessiner un avenir désirable et un horizon d'attente.

La passerelle entre le monde de la recherche académique et le monde politique de la décision publique doit être renforcée.

Mme Marion Lenne. Je trouve que Thierry Breton porte tout de même bien le numérique. De plus, un choix a été fait en France sur le numérique. Nous avons deux ministres ou secrétaires d'État ; nous portons la transformation de la fonction publique au niveau du numérique ; les volets économiques et territoriaux sont portés par Cédric O. Nous sentons donc une volonté politique, mais elle est freinée au plus près des territoires.

Je suis allée à l'inauguration d'une école dernier cri, superbe et quand j'ai demandé si l'école était reliée à la fibre, tout le monde m'a répondu non. Il faut imposer dans les appels d'offres le fait que les écoles soient reliées, notamment au lendemain des assises sur le numérique dans les écoles. Il faut que, dans chaque ministère, de véritables visions soient portées sur le numérique. Nous avons pendant des années mis un poison dans la tête des gens en expliquant que le numérique était le diable.

Cela avance très nettement grâce, hélas, à la crise covid, mais un véritable changement d'état d'esprit vis-à-vis du numérique est nécessaire et nous devons tous le porter. En commission des affaires étrangères, nous étudierons bientôt un rapport sur la création de l'eco, une monnaie pour l'Afrique de l'Ouest : il s'agit de créer encore une monnaie correspondant aux usages des années 1980 alors que la monnaie de demain est sans doute virtuelle. Nous ne le prenons pas en compte.

Je pense que les gens rêvent, mais sont freinés par des conservatismes bien présents dans les territoires.

M. Charles Thibout. Nous rentrons dans un débat politique, au sens noble du terme, dans lequel je ne veux surtout pas m'engager. Tout ceci implique de se poser des questions de politiques publiques. Quel est le plus important, lors d'un arbitrage financier, entre installer la fibre dans une école au fin fond de la Creuse ou désengorger des classes surchargées en embauchant de nouveaux professeurs et en construisant de nouveaux bâtiments ? C'est une décision politique qui se prend avec les citoyens, en fonction de ce dont ils ont envie. Dans ce cadre, je peux comprendre que la question technologique puisse paraître dérisoire par rapport à des problèmes humains, qui se posent toujours avec plus d'acuité.

Le Commissaire Breton joue avec les cartes qu'il a en main, qui sont assez restreintes : la concurrence qui est le maître mot de la Commission européenne, la modération des contenus et des plateformes. C'est un aspect qui me paraît accessoire et même un peu dangereux en fait.

Vouloir penser ces plateformes comme des médias comme les autres ne me paraît pas répondre aux grands problèmes de notre temps, sachant que ces plateformes ont précisément eu comme intérêt la démocratisation de l'information et de l'accès à l'information, au-delà des biais liés aux bulles algorithmiques ou à l'utilisation des données personnelles à des fins publicitaires. Je crains que la Commission européenne ne s'aventure sur un terrain dangereux qui ne profitera pas à grand monde. C'est une opinion personnelle.

M. Pierre-Alain Raphan. Comment impliquer au mieux le citoyen sur ces sujets ? Nous parlons beaucoup d'économie de l'attention, mais moins d'écologie de l'attention même si Yves Citton a fait de très beaux travaux sur cette question.

Nous alimentons tous, dans nos pratiques et nos habitudes de consommation, ces données qui partent outre-Atlantique ou de l'autre côté de la planète. Comment pourrions-nous améliorer la formation de chaque citoyen pour que nous évitions le paradoxe de cette volonté d'une souveraineté numérique alors que nous faisons souvent l'inverse dans notre quotidien ? Nous avons nous-mêmes des outils et des usages qui alimentent de plus en plus ces oligopoles. Cette formation et cette acculturation pourraient-elles passer par du « coup de pouce » – *nudging* – ou autre ?

M. Charles Thibout. Mes idées sur cette question sont extrêmement banales. L'éducation est effectivement la clé, nous n'avons rien fait de mieux depuis que l'homme parle.

Il faut une éducation technique. Éduquer au code existe déjà et doit pouvoir être généralisé. Comprendre comment fonctionne une machine et ce qu'il est possible de faire est très important. Il faut comprendre l'architecture de l'internet, ce qu'est un routeur, un câble sous-marin. Notre génération n'a pas eu cette formation et elle lui manque. Nous sommes obligés de prendre le train en marche.

Il faut aussi une culture de l'utilisation de l'internet, peut-être à enseigner par le biais de l'éducation civique, en l'articulant avec la géopolitique qui est entrée dernièrement dans les programmes de lycée. Sans tomber dans de la propagande ce qui n'aurait plus aucun intérêt, il serait bon de faire comprendre aux enfants quels sont les enjeux, pourquoi tant d'États crient haro sur les grandes entreprises transnationales du numérique.

J'ai été très agréablement surpris par la Convention sur le climat qui s'est tenue récemment. C'était une respiration fort agréable dans notre démocratie et je pense que cette initiative pourrait être réitérée. Il faut réfléchir à ce que nous faisons des propositions qui en émanent, savoir si elles doivent être débattues au sein du Parlement ou transcrites dans l'ordre juridique étatique. C'est à vous de voir.

Multiplier ces débats me semble intéressant, soit de manière institutionnelle cadrée comme la Convention sur le climat soit de façon plus informelle en aidant les associations et les fondations à organiser ce type de rencontre. Nous pourrions avoir des spécialistes du technique, de la science, capables de dire où en est l'état de l'art et doubler par un débat plus citoyen avec des responsables politiques de bords opposés ou des personnes issues de la société civile et engagées sur le sujet.

Ce ne sont pas des idées révolutionnaires, mais sensibiliser les citoyens sans les infantiliser est important.

M. Philippe Latombe, rapporteur. Monsieur Thibout, souhaitez-vous ajouter quelques mots pour conclure ?

M. Charles Thibout. Je redis simplement que, avant de penser un chemin technologique, il faut penser un chemin politique donc définir nos intérêts pour définir des objectifs et en déduire une stratégie.

Audition, ouverte à la presse, de Mme Lorena Boix Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne (19 novembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je vous prie d'excuser notre rapporteur Philippe Latombe qui défend actuellement les amendements dans l'hémicycle. S'il en a la possibilité, il nous rejoindra, mais c'est à moi que revient l'honneur d'accueillir Mme Lorena Boix Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne. Comme vous le savez sans doute, notre mission d'information porte sur les moyens de bâtir et de promouvoir une souveraineté numérique française et européenne. Il nous est donc absolument essentiel de recevoir l'éclairage européen des institutions qui peuvent contribuer à ces mêmes objectifs. Dans le cadre de nos travaux, nous sommes particulièrement sensibles à l'actualité européenne dans le domaine du numérique. Nous avons d'ailleurs initié cette mission en auditionnant Mme Mariya Gabriel, commissaire européenne chargée de l'innovation, de la recherche, de la culture, de l'éducation et de la jeunesse.

Je souhaite vivement que l'audition de ce jour nous permette de comprendre de quelle façon la souveraineté numérique est envisagée, promue et défendue au sein de l'Union européenne. Je pense également qu'il nous serait utile de faire un point d'actualité sur les différents dossiers numériques portés par la Commission européenne concernant la régulation des plateformes et les stratégies de la donnée et de l'intelligence artificielle, qui sont des sujets sur lesquels la Commission est particulièrement engagée.

Mme Lorena Boix Alonso, directrice chargée de la stratégie et de la diffusion des politiques à la Direction générale des réseaux de communication, du contenu et des technologies de la Commission européenne. La souveraineté numérique est d'une importance capitale et fait partie d'un concept plus large, celui de la souveraineté stratégique. Les technologies numériques sous-tendent les évolutions dans tous les secteurs de l'économie, que ce soit l'agriculture, les finances ou la sécurité. Plus généralement, elles déterminent nos capacités à relever les principaux défis sociétaux, comme la santé et l'environnement. N'importe quelle dépendance, même minime, à l'égard de technologies numériques développées et produites en dehors de l'Union européenne pourrait rendre vulnérables ces différents secteurs de notre économie et de notre société. Une dépendance dans le domaine numérique pourrait mettre en péril non seulement notre économie, mais également notre sécurité, nos valeurs démocratiques et nos droits fondamentaux. L'ubiquité des technologies numériques dans l'économie rend particulièrement important le développement de la souveraineté numérique. La crise de la covid a renforcé cette idée en agissant comme une prise de conscience de l'importance de ces enjeux. Cette crise est un drame humain et une crise économique, mais je suis convaincue que ce drame aurait été plus conséquent sans le numérique qui nous a permis de continuer à exercer nos activités économiques et sociales et qui a également aidé à gérer la situation du côté humain, social et médical. Cette fantastique accélération qu'a apportée la covid dans de nombreux secteurs est une opportunité. C'est pour cette raison que vos travaux arrivent au bon moment. Il convient de redéfinir notre approche du secteur numérique. C'est également un grand défi car ceux qui ne s'adaptent pas encourent le risque de devenir hors-jeu, que ce soient des pays, des entreprises ou des écoles.

La pandémie a révélé des défis, mais également des vulnérabilités. Nos sociétés et économies sont exposées aux chaînes d'approvisionnement mondiales et nous sommes vulnérables si nos outils numériques sont complètement conçus, produits et contrôlés ailleurs. L'enjeu n'est pas uniquement économique mais touche également à nos valeurs, que le développement technologique doit respecter. La résilience stratégique de l'autonomie numérique ne consiste pas à nous isoler, mais à défendre nos intérêts stratégiques et nos valeurs. Pour y parvenir, il faut réduire notre dépendance en construisant nos capacités technologiques. Nous devons développer des projets susceptibles d'aboutir à des alternatives européennes dans les technologies et stratégies clés. Il est nécessaire de donner à nos citoyens les moyens d'agir en encourageant nos talents à se développer, puis à déployer et utiliser ces technologies stratégiques essentielles dans l'intérêt commun. L'Europe peut jouer un rôle central dans cette course mondiale à la puissance technologique. Dans le contexte géopolitique actuel, les grandes puissances telles que la Chine et les États-Unis sont conscientes de l'importance que représente cette capacité à gérer ses propres technologies. L'Europe est plus que jamais consciente des implications.

Nous devons développer nos capacités dans trois domaines clés : le secteur des données, qui est fondamental ; la microélectronique et les microprocesseurs, qui sont dans toutes les chaînes de valeurs électroniques ; et la connectivité. Nous possédons deux outils principaux pour y arriver : les investissements et la régulation. Je vais principalement développer ce deuxième point, mais je pense qu'il faut jouer sur les deux. D'après notre présidente, Ursula von der Leyen, la décennie du numérique commence. Elle veut développer l'Europe et a proposé dernièrement ce qu'elle appelle une boussole numérique. Le Conseil européen a appelé la Commission à développer ce concept. En mars 2021, nous proposerons des objectifs chiffrés et clairs pour l'horizon 2030, afin de ne pas présenter uniquement les investissements et la régulation, mais pour nous fixer des buts et mettre en œuvre les moyens pour les atteindre. Je serais très heureuse de développer le concept de souveraineté numérique à l'occasion de nos débats et d'expliquer de manière plus approfondie les différents projets législatifs des prochaines années.

M. le président Jean-Luc Warsmann. Vous avez bien rappelé la déclaration de la présidente de la Commission européenne et sa volonté de faire de la décennie 2020 celle du numérique. Nous avons la sensation que la souveraineté numérique fait l'objet de définitions nationales sensiblement différentes dans un certain nombre d'États membres. Comment la Commission travaille-t-elle pour construire une vision commune dans ce domaine et quelles en sont les premières déclinaisons concrètes au niveau du pouvoir législatif ?

Vous avez parlé de l'aspect réglementaire, j'aimerais aborder le thème de la concurrence. Les GAFAM disposent aujourd'hui d'un pouvoir de marché sans précédent dans un nombre croissant d'activités. Les acteurs européens éprouvent de grandes difficultés à devenir des concurrents efficaces. La régulation des plateformes numériques *via* le *Digital Services Act* et la réforme sur la concurrence européenne sont deux chantiers ouverts par la Commission. Pourriez-vous nous en dire davantage sur les effets de fond espérés et sur le calendrier ?

Mme Lorena Boix Alonso. La souveraineté technologique est un concept très en vogue qui possède de nombreuses définitions. Je considère qu'elle possède deux volets, un interne et l'autre externe. Le volet interne représente la nécessité de développer nos propres technologies, ce qui ne signifie pas que nous les produirons toutes en Europe de façon totalement indépendante. Nous devons développer nos capacités propres pour les technologies stratégiques afin de ne pas être dépendants d'un pays unique. Nous avançons l'idée d'investir ensemble sur de grands projets. Les coûts pour développer des capacités fortes dans certaines

de ces technologies sont considérables. Un pays isolé ne peut faire face aux défis que cela implique compte tenu du poids des investissements. Pour cette raison, la Commission veut que nous y travaillions ensemble. Il est important de parler de ces concepts au niveau national, mais encore plus au niveau européen.

Nous proposons d'effectuer des investissements coordonnés pour certains grands projets tels que la recherche et l'innovation, mais également pour le déploiement de nos capacités numériques. Il est crucial de développer le *cloud* pour établir une infrastructure européenne des données, d'agrandir notre capacité de production des microprocesseurs à faible consommation, de déployer des réseaux 5G le long des axes de transport, de mettre en place des infrastructures de communication ultra sécurisées qui utilisent des méthodes de cryptage quantique, et de progresser sur les supercalculateurs. À titre d'exemple, les supercalculateurs occupent un rôle important dans le développement des vaccins et médicaments. Auparavant, comparer des molécules afin de confectionner un médicament prenait des années, mais le processus a été considérablement accéléré avec l'utilisation de ces machines. Pour autant, le coût d'un superordinateur est colossal. Dans cette optique, nous avons créé EuroHPC (*European High Performance Computing Joint Undertaking* - Entreprise commune européenne pour le calcul à haute performance), une entreprise commune aux pays européens. D'énormes projets peuvent ainsi participer favorablement à la souveraineté technologique que nous devons réaliser ensemble.

Nous disposons actuellement de plusieurs programmes pour financer ces projets. Nous espérons arriver rapidement à un accord entre le Conseil et le Parlement sur le cadre financier pluriannuel. Dans le cadre de la nouvelle facilité pour la reprise et la résilience, pour la première fois, nous avons constaté une prise de conscience de l'importance du numérique avec 20 % des dépenses qui y sont consacrées, c'est-à-dire entre 130 et 140 milliards d'euros sur les deux prochaines années. Nous possédons également deux autres moyens de financement : l'Europe numérique, avec 8 milliards d'euros, et la *Connecting Europe Facility*, qui est davantage centrée sur les réseaux.

Si certains États membres comme la France sont de fervents promoteurs de ces concepts, d'autres pays sont plus réticents. Tout dépend de la définition que nous leur donnons. S'ils sont compris comme la fermeture au commerce international, je pourrais comprendre certaines réticences, mais ce n'est pas le cas.

Le second volet que j'aimerais aborder est le volet externe de la souveraineté technologique. Il s'agit de l'aspect international, qui possède également une dimension défensive. Comme le répète régulièrement le commissaire Thierry Breton, nous devons arrêter d'être naïfs, surtout dans nos relations internationales. Il faut nous protéger des pratiques commerciales déloyales en appliquant les règles internationales, garantir la réciprocité des accès aux marchés internationaux, lutter contre les effets de distorsion des subventions étrangères dans notre marché unique et, comme vous l'avez mentionné, adapter le cadre européen de la concurrence pour garantir qu'il réponde aux défis de la transition verte et de la transformation numérique. Le volet international ne signifie pas uniquement que nous devons être défensifs, avec des concurrences équitables, mais également que nous devons créer des liens avec ceux qui partagent nos valeurs. Nous ne sommes pas complètement isolés.

La présentation du *Digital Services Act* est annoncée pour décembre. L'objectif est de doter l'Union européenne d'un cadre juridique ambitieux pour les services numériques, notamment les plateformes en ligne. Nous voulons parvenir à une harmonisation des règles au niveau européen pour permettre l'essor et l'innovation au sein du marché commun. Le *Digital Services Act* sera accompagné du *Digital Market Act*. Ce dernier essaye de garantir une économie numérique innovante et une compétitivité équitable. Son objectif consiste à tracer

les lignes directrices de cet espace informationnel, dont parle régulièrement notre commissaire, afin de renforcer le marché unique. Lorsque les entreprises proposent leurs services sur le marché, il faut qu'elles soient responsabilisées pour protéger nos citoyens contre les activités illicites.

Ces éléments constituent le cœur du *Digital Services Act*. Ce cadre législatif, d'un côté, permettra une protection juste des citoyens et une garantie de leurs droits et, de l'autre, rendra possible l'émergence d'un secteur numérique robuste et compétitif en Europe. Ce qui est illégal en dehors du web doit également l'être en ligne. Notre idée consiste à créer une série d'obligations de vigilance pour les plateformes en ligne. Pour en citer quelques-unes, nous pensons à des procédures de notification, avec la création d'une procédure en Europe de notification des contenus illicites, ainsi qu'à des mesures de recours, de transparence et de coopération avec les autorités publiques. Ces obligations de vigilance seront renforcées pour les grandes plateformes. En effet, la responsabilité s'accroît en fonction de l'audience.

Les règles actuelles de gouvernance s'appliquent par rapport au pays où est établie la plateforme. C'est un principe valable et important, car une entreprise doit pouvoir choisir où s'installer. Je partage avec vous nos réflexions car cela n'a pas encore été adopté, mais il sera très important d'éviter que les plateformes se cachent derrière un vide juridique. Nous réfléchissons à créer un système de coopération entre toutes les autorités nationales pour éviter ce genre de situation.

Voici les grandes lignes du *Digital Services Act*. Je peux également détailler d'autres propositions législatives si vous le souhaitez. Nous avons en effet plusieurs propositions que nous adopterons prochainement. En décembre, nous aurons le *Digital Services Act* et le *Digital Market Act*. Une autre proposition que j'estime essentielle pour la souveraineté numérique est l'identité numérique. C'est quelque chose que notre présidente a annoncé dans le discours et le débat sur l'état de l'Union et qui figure désormais dans notre programme de travail pour le premier trimestre de l'année prochaine. Nous voulons faire une proposition qui vise à établir un cadre unique pour une identité numérique européenne qui soit universellement reconnue, sécurisée, fiable, et qui puisse être utilisée partout où nous nous identifions sur internet. Cela ne signifie évidemment pas qu'elle remplacera les identités nationales, mais c'est quelque chose qui peut jouer un rôle fondamental. En ce moment, lorsque nous commençons à utiliser un nouveau service sur internet nous rencontrons souvent la demande : « Comment souhaitez-vous vous identifier ? » Nous pouvons entrer notre nom et notre *e-mail*, mais il nous est également proposé de nous identifier en utilisant une plateforme des GAFAM. C'est une méthode d'identification tellement plus facile que nous préférons souvent l'utiliser. Évidemment, se pose alors la question de l'utilisation de nos données. Il serait préférable que nous possédions le moyen d'utiliser une identité numérique alternative qui nous permette de contrôler nos données et de garantir la sécurité. Il est trop tôt pour préciser le contenu de cette proposition, mais c'est l'idée sur laquelle nous travaillons et que nous explorons actuellement.

Un autre enjeu important est celui des données. Nous allons créer un cadre pour la gouvernance des données afin de garantir la solidité et la pérennité des espaces européens communs des données. C'est une idée importante pour notre commissaire. Les GAFAM ont gagné la bataille des données personnelles en développant de nombreuses activités qui leur sont liées, mais l'enjeu pour l'avenir concerne les données industrielles et publiques. L'Europe est très forte dans ce domaine grâce à une industrie et un secteur public puissants. Nous pouvons accomplir beaucoup de choses autour de l'économie de ce type de données industrielles et publiques, d'où l'idée de créer des espaces communs des données. Pour y arriver, il est nécessaire d'établir un cadre réglementaire de gouvernance afin de savoir ce que nous pouvons faire. Je vais donner un nouvel exemple. Avec la pandémie, nous avons réalisé

que les données sont centrales. Nous utilisons les données, comme je l'ai dit précédemment, pour trouver des médicaments et un vaccin, mais également pour mesurer l'évolution de la pandémie et pour évaluer l'impact des mesures prises par les gouvernements. Nous aurions pu accomplir beaucoup si nous avions eu cette coordination des données et cette gouvernance pour savoir ce que nous pouvions en faire et de quelle manière les utiliser. Pour cette raison, nous proposerons très prochainement un cadre de gouvernance des données en Europe, peut-être ce mois-ci. Cela permettra également de libérer la valeur des données mises volontairement à disposition, de faciliter le partage des données de manière contrôlée avec une vision technique, juridique et organisationnelle, et de renforcer la confiance dans ces espaces de données.

Nous préparons également au troisième trimestre 2021 une proposition législative qui vise à améliorer la qualité des données du secteur public, telles que les statistiques et les données géospatiales, afin qu'elles soient disponibles pour réutilisation compte tenu de leur potentiel pour les petites et moyennes entreprises européennes. Nous préparons une loi d'exécution sur l'ensemble des données de grande valeur afin de les rendre réutilisables dans toute l'Union européenne dans des conditions techniques et, dans ce cas-ci, gratuites. Comme vous le constatez, beaucoup d'éléments arriveront sur les données.

Une autre initiative législative, prévue pour le troisième trimestre 2021, est également en discussion. Elle cherche à accroître l'équité dans l'économie des données. Elle visera à clarifier les trois utilisations des données dans les contextes *Business To Business* et *Business To Government*. Premièrement, nous voulons améliorer le droit de portabilité des données afin de donner aux citoyens plus de contrôle dessus. Par exemple, nous voulons être capables d'exercer le droit que nous possédons, mais qui est difficile à mettre en œuvre, de porter nos données ailleurs lorsque nous voulons sortir d'une plateforme. Deuxièmement, nous allons examiner le droit de propriété intellectuelle en vue d'améliorer davantage l'accès à l'utilisation des données. Troisièmement, cette initiative clarifiera l'utilisation des données dans le domaine de la cybersécurité.

Nous réexaminons en ce moment la directive sur la sécurité des réseaux et des systèmes d'information. Nous avons terminé l'analyse d'impact et présenterons une proposition législative idéalement avant la fin de l'année, ce qui me semble être un objectif réaliste.

Enfin, comme vous l'avez mentionné, nous proposerons également pour l'année prochaine un cadre réglementaire pour l'intelligence artificielle où nous essayerons de conserver un équilibre entre, d'une part, l'encouragement de l'innovation et du recours par les entreprises et le secteur public à des solutions d'intelligence artificielle et, d'autre part, la protection de nos citoyens contre les biais parfois indésirables qu'entraînent ces technologies. Nous possédons un programme très intensif, en coopération avec tous les États membres.

M. le président Jean-Luc Warsmann. Nous avons constaté, depuis le début des travaux de la mission, la difficulté d'établir un écosystème public et privé de cybersécurité et cyberdéfense, non seulement sur son aspect réglementation, mais également sur le volet économique. J'avais une dernière question. Pourriez-vous nous apporter un éclairage sur les aspects éthiques de l'intelligence artificielle, de la robotique et des sujets connexes ? Je sais qu'il y a des réflexions à la Commission européenne là-dessus.

Mme Lorena Boix Alonso. Je pense qu'une véritable prise de conscience du besoin important d'investissements dans ces domaines est nécessaire. En Chine et aux États-Unis, les investissements dans la cybersécurité ont augmenté d'une manière radicale ces dernières années. Nous constatons une prise de conscience, comme j'en parlais dans mon introduction, du potentiel énorme du numérique, mais nous pouvons tout perdre si nous ne sommes pas

protégés. La covid a montré de manière très claire l'enjeu. Des hôpitaux ont été attaqués à des moments-clés. Des centres de recherche qui travaillaient sur des vaccins ont également subi des attaques. L'enjeu est donc considérable. Souvent, nous percevons la sécurité comme cantonnée au monde numérique, mais il s'agit d'un sujet tangible et physique. Des personnes peuvent mourir si un hôpital est attaqué. Il s'agit donc d'un problème crucial et il est important d'investir dans la cybersécurité.

Nous possédons plusieurs initiatives au niveau européen. En ce moment, une discussion se tient entre les États membres et le Parlement européen pour la création d'un centre de compétence sur la cybersécurité. Son objectif est de développer l'excellence en matière de cybersécurité avec la participation de tous les États membres et de créer un réseau de communication entre ces centres et les réseaux d'excellence sur la cybersécurité au niveau européen. Leur création est imminente, nous terminons les négociations en ce moment. Beaucoup d'argent entre en jeu puisque 2 milliards d'euros seront apportés par un nouveau programme que nous avons créé, le programme de l'Europe numérique. C'est un programme de près de 8 milliards d'euros qui, pour la première fois, est consacré exclusivement au numérique.

Ces financements seront, pour la première fois encore, consacrés non pas à la recherche, que nous allons évidemment continuer à financer, mais à un élément sur lequel nous n'investissons pas assez en Europe : le déploiement des technologies. Dans le domaine de la recherche, nous sommes parfois très bien positionnés en Europe, comme dans le domaine de la cybersécurité. Nous sommes forts pour investir et pour trouver des technologies magnifiques. Nous possédons des entreprises impressionnantes, mais que se passe-t-il ensuite ? Cette technologie est développée et déployée ailleurs. Nous possédons des exemples de technologies découvertes en Europe qui ont été déployées en Chine ou aux États-Unis. C'est pour cette raison que nous avons créé ce nouveau programme Europe Numérique, afin de financer le déploiement en Europe de ces technologies avec 2 milliards d'euros consacrés au déploiement des nouvelles technologies en matière de cybersécurité. Ces programmes font partie des négociations sur le cadre financier pluriannuel. Nous clôturons actuellement les négociations et je suis très confiante. Évidemment, nous devons continuer à investir pour la recherche et le programme Horizon Europe y consacrera une partie de son budget.

Au niveau de l'intelligence artificielle, comme vous l'avez mentionné, des travaux ont été faits. Nous avons créé un groupe de haut niveau pour développer des directives sur les principes éthiques de l'intelligence artificielle. Ce travail sera pris en compte par la Commission européenne lorsque, l'année prochaine, nous proposerons un cadre réglementaire. Il est très important de trouver un équilibre avec nos valeurs et principes éthiques européens pour ne pas freiner l'innovation. La Commission cherche à garder cet équilibre et je pense que nous avons fait preuve par le passé de notre capacité à apporter des propositions réglementaires pour le maintenir. C'est d'ailleurs pour cette raison que nous sommes copiés par d'autres pays. L'année passée, nous avons proposé la première réglementation sur les plateformes, qui concernait d'autres domaines. Elle a été imitée par la Corée et le Japon. Compte tenu de l'impact que peut avoir l'intelligence artificielle sur nos démocraties et nos droits fondamentaux, nous espérons pouvoir devenir un exemple au niveau international.

M. Denis Masséglia. Je veux revenir sur la question de mon collègue concernant la construction d'une stratégie européenne, à laquelle vous avez répondu. Cette construction stratégique s'effectue à travers différents pays qui, bien souvent, ont tendance à vouloir tirer la couverture à eux. Étant un partisan d'une Europe fédérale, je pense, qu'au moins sur cette partie-là, nous pourrions essayer de mettre en place une stratégie avec un leadership européen

sur de fortes thématiques. Si nous voulions construire le Google de demain, où plutôt une technologie future là où Google est pratiquement une technologie dépassée, comment éviter que chaque pays essaye de tirer la couverture à lui pour mettre en place une stratégie commune ? Les financements pour l'intelligence artificielle en France représentent 1,5 milliard d'euros, alors que la Chine investit vingt fois plus. La seule solution serait que nous combinions les financements de chaque pays européen afin que chacun puisse se saisir d'une brique de construction pour qu'à la fin, nous aboutissions à un ensemble commun. Cet ensemble commun doit être piloté par une entité unique au niveau de la synthèse des travaux. Comment considérez-vous cette proposition ?

Mme Lorena Boix Alonso. Vous avez raison, il existe cette tendance, qui fait partie de la beauté de l'Europe, pour chaque pays membre, à tirer d'un côté lorsque nous parvenons à un accord. Je pense que c'est pour cette raison que nous arrivons souvent à des propositions équilibrées. Je ne connais pas d'autre système où nous mesurons autant tous les intérêts qui sont en jeu.

Dans le domaine de la souveraineté technologique ou numérique, même si un pays voulait devenir leader, ce serait impossible. Comme vous l'avez dit, les sommes d'argent investies par des pays extraeuropéens sont énormes. Aucun État ne peut rivaliser seul. Le seul moyen d'y parvenir est la mise en place de grands projets. J'ai mentionné le *cloud* qui est un bon exemple. Comme nous l'avons constaté, la France et l'Allemagne ont commencé à pousser dans cette direction avec le projet GAIA-X pour créer un système de *cloud* européen. La Commission européenne considère ces projets avec beaucoup de sympathie. Nous sommes en train de lancer une alliance industrielle au niveau européen avec pour objectif la création d'une infrastructure de *cloud*, qu'il serait impossible de créer avec un seul pays. Notre commissaire a participé à un événement sur ces grands projets et GAIA-X. L'objectif est d'être complémentaire et de créer des synergies. L'Europe permet ces coordinations. Je pense que c'est le rôle que peut jouer l'Europe en démarrant et coordonnant ces grands projets, mais aussi d'y participer financièrement quand c'est possible. Nous disposons de plusieurs outils financiers pour lancer ces projets et attirer, grâce à notre intervention, de l'investissement privé. Il faut réaliser cela ensemble avec les États membres, les entreprises et l'Union européenne. Nous ne pouvons qu'en sortir gagnants.

M. Denis Masséglia. J'apporte mon soutien à la Commission européenne contre la volonté de certaines entreprises de vider le *Digital Services Act* de son contenu. Nous sommes avec vous et nous devons mettre en œuvre une stratégie européenne pour protéger nos intérêts. Il y a certes un changement de président aux États-Unis, mais je reste persuadé que la devise *America First* restera malgré tout la politique de nos amis et partenaires américains.

M. le président Jean-Luc Warsmann. Je partage ce message. Nous vous remercions à nouveau et vous souhaitons bonne continuation sur des missions aussi stratégiques que vous portez pour notre Union européenne.

Mme Lorena Boix Alonso. Je vous remercie de donner à la Commission la possibilité d'interagir. Je vous informe également que je viens d'être nommée directrice de la cybersécurité, de la santé électronique et de l'identité numérique. Dans mes nouvelles capacités, ce sera avec plaisir que j'expliquerai ces domaines de manière plus approfondie, si vous le voulez.

Audition, ouverte à la presse, de M. Werner Stengg, membre du cabinet de Mme Margrethe Vestager, vice-présidente exécutive de la Commission européenne, sur « Une Europe adaptée à l'ère du numérique »
(19 novembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je suis très heureux de souhaiter la bienvenue à M. Werner Stengg qui est conseiller au cabinet de la vice-présidente exécutive de la Commission européenne, Mme Margrethe Vestager. Comme vous le savez, notre mission d'intervention porte sur les moyens de bâtir une souveraineté numérique française et européenne. L'action de la vice-présidente contribue à atteindre ces objectifs depuis plusieurs années. Dans le cadre de nos travaux, nous sommes évidemment extrêmement sensibles à l'actualité européenne dans le domaine du numérique. Nous avons d'ailleurs initié cette mission en auditionnant Mme Mariya Gabriel, la commissaire européenne chargée de l'innovation, de la recherche, de la culture, de l'éducation et de la jeunesse. Nous attendons beaucoup des auditions de ce jour. Nous souhaitons mieux comprendre comment la souveraineté numérique est envisagée, promue et défendue au sein de l'Union européenne. Nous souhaiterions également que vous nous fassiez un point d'actualité sur les principaux dossiers numériques portés actuellement par la Commission européenne, notamment en ce qui concerne la régulation des plateformes, ainsi que les stratégies de la donnée et de l'intelligence artificielle qui sont des sujets sur lesquels nous avons déjà lu et entendu des prises de position des travaux de la Commission.

M. Werner Stengg, membre du cabinet de Mme Margrethe Vestager. Je vous remercie pour cette invitation et aux questions que vous avez bien voulu nous adresser. Je ne suis pas certain d'être en mesure de répondre à toutes, notamment concernant à celles concernant la finance numérique et la fiscalité, dossiers sur lesquels je n'ai jamais travaillé. Au sein du cabinet de Mme Vestager, je m'occupe des plateformes, de l'intelligence artificielle et de la politique sur les données. Je vais donc, si vous le permettez, me concentrer sur ces dossiers. J'ai également beaucoup travaillé sur la stratégie numérique des commissions européennes successives.

Comme vous le savez, nous avons commencé à communiquer sur notre stratégie en février, avant la covid. Nous avons déjà abordé la question de la souveraineté qui est un thème horizontal multidimensionnel. Notre point de départ consiste à savoir comment l'Europe peut façonner la manière dont la transformation numérique nous concerne. Notre premier constat est que nous ne sommes pas uniquement des victimes de la transformation digitale, à laquelle nous devons nous adapter annuellement, mais que nous possédons également les moyens et la volonté politique pour la façonner. Toutes les entreprises européennes, tous les citoyens, et la société en général peuvent en bénéficier.

Je vais commencer par définir ce que nous entendons par souveraineté technologique. C'est un domaine qui concerne l'intégrité de notre infrastructure, de nos réseaux, des infrastructures de données, des communications et des technologies en général. Si nous ne sommes pas en mesure de gérer nous-mêmes toutes ces technologies, alors nous n'aurons pas la chance de pouvoir les influencer. Par exemple, si pour un dossier clé tel que l'intelligence artificielle nous n'arrivons pas à devenir un acteur important dans son développement, il sera difficile de nous assurer que nos valeurs soient mises en avant. En étant seulement consommateurs de cette technologie, il sera en effet compliqué de refuser de l'utiliser si des

éléments ne nous conviennent pas. Nous devons être forts et indépendants. Ce n'est pas une question de protectionnisme, mais d'indépendance et de compétitivité de notre industrie.

La nouvelle vague de la transformation concerne les données et l'intelligence artificielle. Nous ne voulons pas encore une fois être en retard par rapport aux Américains. Comme vous le constatez également dans vos questions, aujourd'hui, nous n'avons pas réussi à développer les services visant les consommateurs tels que les grandes plateformes. Cependant, nous pouvons réussir dans la prochaine étape, celle des données et de l'industrie. Le grand moteur de l'Europe a toujours été l'industrie, les petites, moyennes et grandes entreprises. Beaucoup de données sont créées quotidiennement, ce qui représente une ressource considérable. Nous voulons être en mesure de bénéficier de ce développement. Par exemple, nous voulons mettre ces données et les technologies qui y sont liées à la disposition des entreprises et des chercheurs. L'enjeu n'est pas uniquement économique, mais également sociétal. La recherche sur les données nous permettra d'améliorer notre système de santé et de nous battre contre le réchauffement climatique. Le potentiel est énorme pour l'industrie, les entreprises et la société, à condition d'être en mesure de maîtriser toutes ces technologies et de développer les infrastructures qui y sont liées. Nous avons besoin d'une bonne connectivité avec des infrastructures pour partager ces données, mais toujours d'une manière qui corresponde à nos règles et valeurs. C'est donc également une question de confiance, non seulement auprès des citoyens, mais également auprès des entreprises qui envisagent peut-être de partager et d'utiliser les données. Nous devons ainsi établir des règles très claires pour bien protéger nos droits et nos valeurs.

Avec la crise de la covid, nous avons réalisé que, de plus en plus, nous sommes tous dépendants des technologies numériques. Les entreprises doivent les utiliser pour vendre leurs produits car, dans une situation de confinement, c'est la seule façon de trouver des consommateurs. Le gouvernement s'en sert pour fournir des services de base. Les consommateurs les utilisent également. Pourtant, nous dépendons de grandes entreprises, principalement américaines, mais également chinoises. Celles-ci ont été renforcées par la crise car toute la vie économique et privée s'est déplacée sur le monde numérique.

À côté de la souveraineté technologique, le deuxième aspect que je veux aborder est le volet législatif. Au sein de notre Commission, nous prenons beaucoup de mesures pour nous assurer que les grandes entreprises numériques, mais également tout le monde numérique, respectent des règles claires. Les deux initiatives principales que nous publierons le 9 décembre seront le *Digital Services Act* et le *Digital Market Act*.

Le *Digital Services Act* remplacera le cadre établi depuis vingt ans avec la directive sur le commerce électronique. En 2000, nous connaissions déjà Google et un petit peu Amazon, mais tous les services numériques que nous utilisons aujourd'hui et les entreprises qui les fournissent n'existaient pas. Beaucoup d'éléments positifs résultent de ces plateformes : les entreprises peuvent les utiliser afin de trouver des consommateurs plus facilement ; les consommateurs ont accès à un vaste choix de produits et de services à des prix, peut-être, moins élevés qu'avant ; tout le monde peut partager des informations et participer aux débats démocratiques. Nous voulons conserver tous ces avantages. Nous avons néanmoins constaté différents problèmes liés à ces *business models* : des produits placés sur notre marché qui n'atteignent pas nos standards de qualité, ne respectent pas nos normes de sécurité, ou qui sont contrefaits ; des discours haineux et l'apologie du terrorisme. Ainsi, beaucoup de problèmes ne sont pas traités dans le cadre législatif défini par la directive sur le commerce électronique. Nous connaissons aujourd'hui les risques liés à ces services. Avec le *Digital Services Act*, nous allons créer un cadre clair avec des responsabilités pour tous les fournisseurs de ces services numériques, de façon à nous assurer que leurs activités ne mettent pas en danger la

société, les consommateurs et les citoyens. Il est nécessaire de mettre en place des obligations nettes destinées aux entreprises numériques, notamment les plus importantes. En effet, là où les risques sont les plus prononcés, les obligations doivent être les plus grandes. Je vais donner un exemple qui concerne la démocratie. Quand les grandes plateformes qui gèrent nos informations en ligne prennent une décision, qui nous concerne tous, nous ignorons sur quelle base elle est prise. Ils mettent en place des systèmes de recommandation pour nous donner accès à des informations spécifiques. Pourtant, nous ne savons pas sur quels critères nous sommes ciblés par ces informations et pourquoi nous n'en voyons pas d'autres. Ce flou est négatif et, à l'extrême, peut même exercer une influence sur nos élections. Nous travaillons donc beaucoup pour établir des règles claires et nous diriger vers plus de transparence et de redevabilité.

Le deuxième aspect du *Digital Services Act* concerne l'application des règles déjà existantes. Dans le monde numérique se passent beaucoup d'activités illégales, mais il est très difficile d'y appliquer les règles. Il faut donc renforcer la coopération entre les autorités, qui mettent en œuvre la législation nationale, et les plateformes, souvent établies dans un autre pays membre. Nous devons également établir des règles claires pour savoir comment donner un ordre à une plateforme et quelles informations nous pouvons lui demander. La plateforme sera évidemment obligée de fournir ces informations. Il est également nécessaire de renforcer la coopération entre les États membres et la Commission pour protéger le marché intérieur. Notre objectif est l'établissement d'un vrai marché intérieur pour les services numériques fondé sur une responsabilité accrue de tous les acteurs et une meilleure coopération entre les autorités dans la mise en œuvre des règles. Ce marché intérieur reste un moteur clé de promotion des acteurs européens. Il a toujours été le point le plus fort de l'Europe et, si nous voulons des entreprises numériques européennes qui grandissent et entrent en concurrence dans d'autres pays tiers, il faut le préserver.

Avec le *Digital Market Act*, nous visons la mise en place d'un marché intérieur plus sûr et transparent où la concurrence peut avoir lieu. Avec l'émergence des grandes plateformes, nous avons assisté à une dynamique néfaste à la concurrence. Quelques plateformes sont devenues tellement importantes que tout le reste de l'économie dépend d'elles. Des entreprises doivent, d'un côté, travailler avec ces plateformes pour trouver des consommateurs et, de l'autre, entrer en concurrence avec elles. Il leur est presque impossible de se passer du pouvoir de marché accru que permettent ces plateformes. Avec le *Digital Market Act*, nous nous focalisons sur quelques entreprises qui jouent ce rôle crucial dans l'économie. Très souvent, ces plateformes gèrent des marchés qu'elles ont créés : des *appstores*, des *marketplaces,* des moteurs de recherche, des réseaux sociaux. Nous dépendons tous de ces marchés, mais ce sont ces plateformes qui seules édictent les règles et disposent de toutes les informations. Elles peuvent ainsi prendre des décisions sans aucun contrôle extérieur, notamment des autorités. Souvent, elles fournissent leurs propres services à travers ces marchés. C'est l'occasion d'utiliser toutes les informations à leur disposition pour donner la préférence à leur propre service. Elles utilisent beaucoup d'autres méthodes qui rendent plus difficile la vie des entreprises qui dépendent d'elles ou qui veulent entrer en concurrence avec elles.

Ce *Digital Market Act* établira des critères pour identifier ce type d'entreprise. Lorsqu'une entreprise répond à ces critères, des choses lui deviennent interdites. À travers des listes blanches, noires et grises, nous décrivons les prohibitions et obligations à respecter par ces grandes plateformes numériques. Je pourrai entrer plus en détail sur chaque dossier en fonction de vos questions ultérieures. Voici les deux propositions législatives majeures qui nous attendent.

Comme je le disais précédemment, nous possédons également une stratégie sur les données pour que nous bénéficiions tous des données créées quotidiennement. Nous ne parlons pas seulement des données personnalisées, mais également des données industrielles ou mixtes. Comment créer un cadre pour mieux profiter de cette richesse que représentent les données ? La première étape, peut-être la semaine prochaine, portera sur la gouvernance des données. L'objectif n'est pas, pour le moment, d'établir des obligations de partage des données, mais plutôt de créer les infrastructures dont nous aurons besoin lorsque nous voudrons créer de réels espaces de données européens. Si, l'année prochaine, nous voulions construire des espaces européens dans les domaines de la santé, de l'industrie ou encore de l'agriculture, il faut créer des structures de confiance. Imaginez qu'un groupe d'entreprises ou de chercheurs veuille partager un tel espace de données. Celles-ci doivent être stockées quelque part. Elles doivent être placées dans les mains de quelqu'un qui suit des règles très claires de gouvernance des données. Si, en tant qu'entreprise, je souhaite mettre mes données en commun avec d'autres pour bénéficier de la totalité des données, je ne veux pas que l'intermédiaire les utilise à d'autres fins. Il faut établir une claire séparation de l'activité. Un intermédiaire qui héberge ces données ne peut faire autre chose que mettre cette infrastructure à disposition des participants. Il doit protéger ces données. Certaines peuvent être confidentielles et il faut rassurer les entreprises sur le fait qu'elles ne seront pas utilisées à d'autres fins et qu'elles sont sécurisées. C'est un point que nous abordons dans cet acte de gouvernance.

Vers la fin de l'année prochaine, nous proposerons un deuxième acte législatif, le *Data Act*, où nous aborderons des questions plus spécifiques sur les moyens de promouvoir le partage des données et sur leur portabilité. Nous nous demandons, par exemple, s'il existe des domaines où le partage des données doit être obligatoire ou, au contraire, des domaines où le partage avec le public doit être interdit. Nous aborderons ces questions difficiles l'année prochaine.

Pour terminer ce tour d'horizon des propositions importantes, j'aborderai notre travail sur l'intelligence artificielle. Vous avez tous lu le livre blanc paru ce printemps. Nous le traduisons actuellement en actions législatives pour répondre aux problèmes posés par l'intelligence artificielle à haut risque. Nous avons organisé une consultation dans le cadre de laquelle nous avons reçu beaucoup de contributions. Nous ferons une proposition vers la fin du premier trimestre 2021 pour rassurer tout le monde sur les hauts risques de l'intelligence artificielle au niveau de la sécurité, la discrimination, la protection de nos droits fondamentaux. Nous établirons des règles claires pour, d'un côté, être plus transparents afin que chacun comprenne sur quelles bases sont prises nos décisions et, de l'autre, éviter que les résultats de ces machines aboutissent à une discrimination ou à une violation de nos droits fondamentaux.

Je ne m'occupe pas personnellement de la fiscalité numérique, mais nous avons dit qu'à la fin de l'année, nous travaillerons dans le cadre international. Si cela n'aboutit pas, nous proposerons quelque chose nous-mêmes, possiblement pendant la première moitié de l'année prochaine. Les travaux sont en cours et nos collègues de la Commission évaluent actuellement les options dont ils disposent. Je n'ai pas d'information supplémentaire à apporter.

M. le président Jean-Luc Warsmann. Vous avez, au cours de votre intervention, commencé à évoquer les problèmes de position extrêmement dominante des GAFAM et des possibilités d'essayer d'aider à l'émergence de concurrents européens. Vous avez dit au détour d'une phrase que vous pourriez entrer davantage dans les détails. Pourriez-vous nous apporter plus d'informations ? C'est un sujet sur lequel notre mission travaille beaucoup.

Deuxièmement, avez-vous eu l'occasion de travailler sur la cybersécurité et la cyberdéfense, qui sont des domaines qui nous paraissent particulièrement importants ? Quelles

sont les conditions à créer pour développer un écosystème public et privé qui permette de renforcer les atouts européens en matière de cybersécurité et cyberdéfense ?

M. Werner Stengg. Je ne peux malheureusement pas répondre à cette seconde question car je ne suis pas en charge de ce dossier. La cybersécurité est une très grande priorité et un « paquet » est prévu pour la fin de l'année.

Concernant les GAFAM, l'instrument le plus pertinent est le *Digital Market Act*. Ils sont également concernés par le *Digital Services Act*, mais la question centrale n'est pas leur pouvoir de marché, mais plutôt l'impact négatif qu'ils peuvent exercer sur la société. Une grande entreprise comme AliExpress qui transporte des centaines de milliers de colis depuis la Chine possède un impact évidemment bien supérieur à celui d'une petite plateforme. Sur Facebook ou Twitter, d'éventuelles manipulations d'élections ou le partage de discours haineux possèdent un impact considérable. Des régulations plus strictes sont donc mises en place pour ces grandes plateformes. Nous y trouvons donc déjà une dimension concurrentielle. Si vous êtes une entreprise européenne, que vous soyez en ligne ou non, vous devez respecter nos règles et nos normes, c'est-à-dire que vous ne pouvez pas vendre des produits qui ne respectent pas nos acquis communautaires sur la protection des consommateurs et que vous devez payer des taxes. Pour autant, vous êtes en concurrence avec Amazon, Alibaba et Ebay, avec des produits qui viennent de l'étranger, et notamment de la Chine, qui ne respectent pas ces règles et des entreprises qui ne payent pas de taxe. En augmentant la responsabilité des plateformes à travers ces importations, en retirant du marché des produits illégaux, vous n'êtes plus en concurrence avec autant de produits contrefaits ou non sécurisés. Nous avons défini des critères neutres pour déterminer les entreprises couvertes par le *Digital Market Act*. Les GAFAM y répondent, mais également d'autres entreprises seront concernées.

Le *Digital Market Act* est le moyen principal pour améliorer la situation actuelle. Une de vos questions dans votre questionnaire portait sur notre expérience dans la législation des plateformes. Nous en avons peu puisque nous avons commencé au mandat précédent, mais j'avais moi-même négocié le règlement promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne, dit « *Platform to Business* ». De nombreux vendeurs dépendent des plateformes, par exemple les hôtels dépendent de booking.com, les PME dépendent d'Amazon, les développeurs des applications dépendent de l'Apple Store et du Google Play Store. Nous avions commencé à introduire davantage de transparence dans les méthodes de travail de ces plateformes, mais nous avions également accru la possibilité pour les entreprises de contester les décisions prises par elles. Je parle, par exemple, du cas où votre produit est retiré de la plateforme cinq semaines avant Noël sans que vous ne sachiez pourquoi et sans recours possible. Nous avions abordé ces points dans ce règlement. Politiquement, c'était un pas important pour lancer cette dynamique en Europe. Quand nous avions commencé la préparation de cet acte législatif, la moitié des États membres considéraient que nous n'avions pas réellement besoin d'un règlement sur les plateformes. Nous avions alors discuté avec beaucoup de PME dont les représentants craignaient que nous tuions ce modèle, qui était le seul moyen pour elles de vendre dans toute l'Europe et ailleurs, car elles ne possédaient pas les infrastructures pour le faire elles-mêmes. Nous avions au départ rencontré beaucoup d'opposition, mais au fur et à mesure des négociations, presque tous les États membres ont compris que quelque chose avait changé dans notre monde et notre économie et que nous devions en tenir compte. Le Parlement européen a également beaucoup appris de cette expérience. Les questions liées au numérique sont parfois très techniques et tout le monde ne se sent pas tout à fait à l'aise. Mais, après deux ans de négociation avec le Parlement et les États membres, tout le monde a mieux saisi les enjeux. C'était la première fois dans le monde qu'une telle réglementation a été établie. En parallèle, nous avons observé les actions de Mme Vestager dans le monde de la concurrence avec l'application de la loi sur

la concurrence. Nous avons également beaucoup appris à travers ces investigations sur les manières dont travaillent les grandes entreprises, mais nous avons également constaté que cet instrument possède des limites. Après quatre ou cinq ans d'investigation, de nouvelles problématiques sont apparues et d'autres entreprises ont disparu. Ce sont ces deux leçons du mandat dernier qui nous ont menés à franchir la nouvelle étape. Lorsque je consulte les États membres et les membres du Parlement européen, c'est devenu un élément que, je pense, tout le monde appuie.

Mme Virginie Duby-Muller. J'ai une question pointue sur la musique en ligne. Dans le cadre de la préparation des textes *Digital Services Act*, est-ce que vous travaillez à l'évolution du régime actuel de responsabilité limitée des services passifs, inscrit à l'article 14 de la directive sur le commerce en ligne ? L'intervention de la Commission en la matière ne risque-t-elle pas d'aboutir à un affaiblissement généralisé de la responsabilité de certaines plateformes, à l'opposé de l'objectif affiché ? Peut-on, au contraire, espérer un renforcement du rôle de ces services notamment en matière de lutte contre le piratage ? Par exemple, dans le secteur de la musique enregistrée, plus de 88 % des procédures de notification et demandes de retraits de contenus illicites portent sur des contenus déjà notifiés au même service.

M. Philippe Gosselin. Je voudrais vous faire part, dans le cadre du *Digital Services Act*, d'une crainte de déresponsabilisation des hébergeurs en mettant peut-être à leur charge un mouvement d'autolimitation et d'autorégulation qui conduirait en réalité plutôt à un effet de déresponsabilisation. Cela fait partie des éléments qui ont « fuité » ces derniers temps, à tort ou à raison, et je voulais à mon tour poser cette question-là qui est peut-être un peu plus étroite que celle de ma collègue, mais qui me semble dans le même esprit.

M. Werner Stengg. Le but principal de ce projet est de responsabiliser les acteurs, pas de les déresponsabiliser. J'espère que nous atteindrons cet objectif. Si vous examinez le régime actuellement en vigueur, la directive sur le commerce électronique, la responsabilité est un mécanisme très indirect, d'où son manque d'efficacité. La directive prévoit que les plateformes ne sont pas directement responsables. Elles doivent agir lorsque des agissements illégaux leur sont signalés. Elles peuvent décider de ne pas le faire et d'accepter le risque de ne plus être protégé par l'article 14 et donc, éventuellement, d'être pénalisées devant un tribunal. Nous allons renverser ce mode de fonctionnement. Dorénavant, en plus de conserver le risque pour les plateformes de devenir responsables de cette manière, nous allons définir des obligations directes. Les plateformes devront avoir un système de notification et retrait, agir en cas de comportement illégal et suivre des procédures, le tout avec plus de transparence. Les *marketplaces* devront mieux identifier les vendeurs qui utilisent leur plateforme. Souvent, nous rencontrons le cas où une autorité sait qu'un vendeur chinois vend à travers Amazon en Europe. Celui-ci disparaît et se réinscrit à la plateforme pour continuer à vendre. Avec de tels mécanismes, nous exercerons plus de contrôle sur l'identité des vendeurs qui utilisent les plateformes et nous pourrons implémenter des systèmes pour empêcher qu'une même entreprise se réinscrive plusieurs fois.

Le *Digital Market Act* contient également des règles concrètes sur la coopération avec les autorités concernant, par exemple, le transfert d'information et l'obligation de répondre aux ordres donnés. Ces obligations positives visent à montrer le sérieux de ces plateformes dans le combat contre les contenus illicites. Si elles ne sont pas respectées, les plateformes seront pénalisées. En parallèle, l'ancien système reste en place. Si, malgré les efforts et les systèmes mis en place, du contenu illicite apparaît, la plateforme aura à agir rapidement sous peine de devenir responsable juridiquement. L'un ne remplacera pas l'autre, les deux risques seront présents pour les plateformes.

M. Philippe Gosselin. Merci, cela répond à ma question. Nous verrons les modalités et le détail, mais le principe me paraît clair. Concernant le *Digital Services Act*, il a été dit que nous devions avoir une présentation publique le 9 décembre. Est-ce que cette date est confirmée ?

M. Werner Stengg Au début, nous avions prévu la date du 2 décembre pour présenter les deux projets en même temps, mais nous avons pris un peu de retard sur le deuxième. La date du 9 décembre est confirmée.

M. le président Jean-Luc Warsmann. Vouliez-vous aborder d'autres sujets devant notre Commission ?

M. Werner Stengg. Non, je serais plutôt intéressé par votre propre appréciation du sujet, et savoir si nous aurions dû aborder certains sujets différemment.

M. le président Jean-Luc Warsmann. Nous sommes dans une logique de soutien aux démarches de la Commission européenne. Vous avez rappelé l'évolution depuis le mandat précédent. J'avais travaillé sur ces sujets-là lors du précédent mandat et nous avions l'impression d'être très loin de l'opinion majoritaire en Europe à la Commission. Nous considérons que l'évolution est très positive. L'analyse que vous avez eue en détail sur les GAFAM correspond tout à fait à la réalité. La conception que nous avons en France de la souveraineté numérique ne correspond pas à celle de tous les pays européens. C'est exactement, avec des mots différents, ce que vous avez dit tout à l'heure. Il faut un travail de pédagogie.

M. Werner Stengg. Vous dites qu'en France, votre définition de la souveraineté numérique est différente. Quelles sont les différences entre votre conception et celles d'autres pays membres ?

M. le président Jean-Luc Warsmann. Nous avons l'impression que d'autres pays membres adoptent davantage l'attitude que vous avez évoquée, en faisant passer en premier la liberté d'action du privé au détriment des intérêts européens stratégiques de santé, de données et économiques avec l'abus de position dominante des GAFAM. Nous avons l'impression que certains pays se demandent quelle conséquence aurait un raidissement de l'Europe. Nous avons le sentiment que nous jouons notre avenir et la crise de la covid a encore montré à quel point le sujet était sensible. J'ajoute également que je dois vous présenter des excuses, car notre collègue Philippe Latombe, notre rapporteur, est actuellement à l'hémicycle pour défendre des amendements.

M. Philippe Gosselin. J'approuve ce que vous venez d'énoncer. Je suis d'accord avec le fait que nous avons encore aujourd'hui des divergences et des différences de perception sur la souveraineté numérique et notre rapport au numérique extra-européen, notamment les GAFAM. Il y a des divergences très profondes car, en plus de l'aspect économique, elles sont culturelles. Je considère, comme Jean-Luc Warsmann, que nous avons quand même, grâce à la crise actuelle, à toute chose malheur est bon, une conscience qui converge non pas vers une souveraineté nationale, qui aurait un sens limité, mais vers une souveraineté européenne car nous partageons un espace culturel et économique avec des valeurs communes qui valent la peine d'être mises en avant. C'est justement cette notion de valeur commune qui fait qu'aujourd'hui encore subsistent des divergences. De grands progrès ont été réalisés ces dernières années, notamment avec le RGPD (règlement général sur la protection des données), dont la France a été motrice, le *Privacy Act* et les études d'impact. Un corpus devient de plus en plus cohérent, ce qui commence à me rendre enthousiaste.

M. le président Jean-Luc Warsmann. Pour votre information, notre collègue Philippe Gosselin représente depuis des années l'Assemblée nationale à la Commission nationale de l'informatique et des libertés en France, qui existe depuis 1978. Il possède une compétence, une connaissance et une sensibilité à ces sujets particulièrement développées.

M. Philippe Gosselin. Je n'ai pas dit cela, en effet, par hasard car je suis commissaire à la CNIL depuis presque dix ans maintenant.

M. Werner Stengg. Au début de ce mandat, nous avons apporté un ensemble de valeurs et de règles qui sont le fondement de notre stratégie numérique. Quand je disais « *shaping Europe stages the future* », cela signifiait que notre point de départ est constitué de nos valeurs et de nos règles. Je crois qu'avec la covid, cela s'est encore plus accentué. Une autre dimension est celle de la résistance. Au début, nous disions qu'il faut être indépendant et fort pour imposer nos valeurs. Maintenant, nous avons aussi pu assister à la dépendance d'autres pays d'autres régions du monde. Sur le plan technologique également, nous devons nous renforcer pour ne pas être dépendants lorsque nous voulons nous-mêmes fournir les technologies. Je dis cela pour apporter une certaine nuance au concept de souveraineté numérique. Nous pouvons avoir de grands débats politiques sur la souveraineté numérique, être d'accord ou non, mais nous verrons négociation après négociation si les États membres nous suivent ou non. Lorsque nous parlons de gouvernance de données, nous nous demandons s'il y a des données qui ne doivent pas être partagées avec les pays tiers. Sur le sujet de l'intelligence artificielle, nous ne sommes pas protectionnistes, mais si quelqu'un veut placer un produit fondé sur l'intelligence artificielle sur notre marché, il devra respecter les mêmes règles que les nôtres.

Dans tout ce que nous faisons, l'aspect souveraineté apparaît. Les entreprises couvertes par le *Digital Market Act* et le *Digital Services Act* sont surtout originaires de pays tiers. Ce n'est pas par protectionnisme, mais parce que les grandes entreprises ne sont pas européennes. Les grandes entreprises européennes auront également à respecter ces règles. Nous verrons dans les mois et années qui viennent si ce que nous proposons arrive à maturité. J'ai assisté à beaucoup de discours, négociations et réunions de Mme Vestager, qui a toujours trouvé un écho très positif. J'ai l'impression que les choses se dirigent dans la bonne direction.

M. le président Jean-Luc Warsmann. Nous partageons cette impression. Nous vous remercions de cet échange très intéressant.

Audition, ouverte à la presse, de représentants de la Fédération française des télécoms et du groupe de télécommunications Iliad : M. Olivier Riffard, directeur des affaires publiques de la Fédération française des télécoms, M. Anthony Colombani, directeur corporate de Bouygues Telecom, Mme Claire Perset, secrétaire générale adjointe de SFR et Mme Ombeline Bartin, responsable des relations institutionnelles de Free mobile

(26 novembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je suis très heureux d'accueillir aujourd'hui la Fédération française des télécoms (FFT) qui rassemble Bouygues Telecom, Orange et SFR, ainsi qu'un représentant de Free mobile. La Fédération française des télécoms est représentée par M. Olivier Riffard, directeur des affaires publiques, Bouygues Telecom par M. Anthony Colombani, directeur corporate, SFR par Mme Claire Perset, secrétaire générale adjointe et Free mobile par Mme Ombeline Bartin, responsable des relations institutionnelles.

Cette audition s'inscrit dans le cadre des réflexions que nous souhaitons avoir sur la souveraineté de nos infrastructures numériques. La mise en œuvre du déploiement fixe et mobile, la 5G, la protection des infrastructures contre les risques de sécurité constituent des enjeux sur lesquels nous travaillons. Nous sommes évidemment intéressés par l'ensemble des éléments relatifs à la crise de la covid-19 dans votre secteur d'activité.

M. Philippe Latombe, rapporteur. Nous aimerions vous entendre sur plusieurs sujets et d'abord sur le sens qu'a pour vous la notion de souveraineté numérique au sein de votre secteur d'activité. Ce concept est parfois rapproché de celui d'autonomie. Il désigne une forme d'indépendance, de capacité à maîtriser son destin numérique, de ne pas subir les contraintes imposées par certains acteurs publics tels les États ou privés comme les géants du web (GAFAM). De votre point de vue, de quelles façons cet impératif peut-il trouver une ou des traductions opérationnelles concrètes ?

Je souhaite aussi revenir avec vous sur les enjeux relatifs au déploiement des réseaux fixes et mobiles. La souveraineté numérique recoupe en effet directement la question de l'accès aux réseaux de communication électronique. L'objet de nos interrogations est de nous assurer précisément qu'aucun risque systémique ne puisse venir en entraver le bon fonctionnement. Nous aimerions donc vous entendre non seulement sur l'état des déploiements en lien avec le plan France Très Haut Débit et le « New Deal mobile » mais aussi sur la nature et le type des risques de sécurité qui pourraient affecter nos infrastructures à l'avenir ainsi que sur les moyens de s'en prémunir.

Nous souhaitons également échanger sur la 5G. Les enchères viennent de s'achever pour la bande des 3,5 gigahertz et des offres commerciales ont été lancées. Dans ce contexte, alors qu'un régime d'autorisation spécifique a été mis en place par le législateur pour ces équipements, nous aimerions beaucoup entendre votre opinion sur ce sujet, avec la diversité évidente de points de vue qui vous caractérise.

Enfin, nous travaillons également, au sein de cette mission, sur les aspects économiques de la souveraineté numérique. Ils concernent aussi bien la fiscalité que l'émergence d'acteurs français ou européens capables de lutter à armes égales avec nos concurrents extra-européens. Votre regard sur le marché des télécommunications en France et

en Europe, très éclaté me semble-t-il, et sur ses possibles dynamiques à venir nous sera une aide précieuse.

M. Olivier Riffard, directeur des affaires publiques de la Fédération française des télécoms (FFT). La Fédération française des télécoms a été fondée en 2007. Son objectif est de représenter l'ensemble des 17 opérateurs membres – des opérateurs grand public et des opérateurs d'entreprises – et de promouvoir le secteur dans le cadre d'une régulation ouverte. L'exemple typique en est, depuis deux ou trois ans, le « New Deal mobile », un déploiement animé et promu par la Fédération. Ce sujet n'est pas du tout concurrentiel, ce qui nous permet d'être extrêmement mobilisés.

Les services de télécommunication représentent actuellement en France 2 % du produit intérieur brut (PIB). En 2019, 9 gigas de données ont été consommés en moyenne par mois par les mobiles. Nous avons 30 millions d'abonnés au haut débit. Notre secteur représente 51 % du chiffre d'affaires de l'économie numérique, 74 % des emplois, 82 % des investissements et, malheureusement, 83 % des impôts et taxes, ce qui fait le lien avec vos questions sur la fiscalité, notamment vis-à-vis des GAFAM.

Vous avez demandé quelles sont les conséquences de la crise sanitaire sur nos déploiements. Pour la partie haut débit et déploiement de la fibre, nous en étions en 2019 à 4,8 millions de lignes déployées et l'objectif pour 2020 était de dépasser la barre des 5 millions compte tenu du rythme de croisière très important constaté. La crise sanitaire a conduit à l'arrêt pendant plusieurs semaines de l'économie. Nous atteindrons finalement en 2020 un objectif quasiment similaire à celui de 2019 et nous arriverons à 4,8 ou 4,9 millions de lignes déployées.

Malgré toutes les difficultés, le secteur des télécoms n'a jamais arrêté de déployer. Le rythme est tombé très bas pendant le premier confinement mais, contrairement au secteur des bâtiments travaux publics (BTP) et d'autres qui étaient à 90 % à l'arrêt, nous avons toujours maintenu un rythme de déploiement de l'ordre de 20, 30 ou 40 %. Nous avons très vite réussi à remonter, d'abord parce que nous avons anticipé la situation dès le début du confinement, de telle sorte que les salariés disposent très rapidement des protections indispensables pour aller sur le terrain. Nous avons été beaucoup soutenus par les parlementaires et le Gouvernement, ce dont je les remercie. Nous avons obtenu des dérogations pour que les salariés des télécoms soient reconnus comme des acteurs essentiels, puissent se déplacer pour assurer la maintenance des réseaux. Enfin, les opérateurs ont donné un peu de visibilité et de trésorerie à leurs sous-traitants pour qu'ils ne fassent pas défaut.

Au 30 juin dernier, 26 millions de locaux étaient éligibles aux services très haut débit. Nous comptions 12,6 millions d'abonnements avec une progression de près de 600 000 abonnés. La dynamique est donc maintenue. Nous avons réussi à éviter de prendre du retard. Nous ne sommes malgré tout pas encore à 100 % parce que nous avons mis en place des protocoles sanitaires extrêmement stricts. Par exemple, trois personnes ne peuvent plus être présentes en même temps dans un véhicule lors des déplacements. Le but est de maintenir ce rythme élevé, avec actuellement entre 14 000 et 15 000 lignes déployées chaque jour pour la fibre.

Le déploiement mobile s'est maintenant industrialisé avec une architecture inédite où, pour la première fois, le Gouvernement et les parlementaires ont fait le choix du partenariat. Les quatre opérateurs se sont engagés à mettre 3 milliards d'euros dans l'infrastructure mobile pour résorber les zones blanches le plus rapidement possible, en contrepartie du fait que l'État ne renouvelait pas les fréquences 4G, ce qui leur a permis d'économiser 3 milliards d'euros. Les effets en sont maintenant tangibles.

Le « New Deal mobile » comportait plusieurs volets. Le premier était que les opérateurs s'engageaient à basculer tous leurs sites mobiles en propre en 4G d'ici la fin de l'année 2020. Actuellement, la plupart des opérateurs sont quasiment à l'objectif, c'est-à-dire que l'ensemble de leurs sites en propre ont été basculés en 4G avec un peu d'avance.

D'autre part, un dispositif de couverture ciblée avait été négocié dans lequel les collectivités identifiaient des zones prioritaires que les opérateurs avaient l'obligation de couvrir dans les deux ans. Depuis juillet 2018, les collectivités ont identifié plus de 2 000 zones à couvrir. Les opérateurs ont l'obligation d'y déployer un pylône, le plus souvent mutualisé à quatre opérateurs, les arrêtés étant publiés trois ou quatre fois par an. L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) et le Gouvernement ont fait le premier bilan début octobre. Les opérateurs ont atteint l'objectif de déploiement du nombre de pylônes, sauf pour une vingtaine de pylônes qui n'ont pas pu être installés dans les délais. Les raisons en sont soit des difficultés liées à des oppositions de riverains soit des difficultés liées à l'absence d'autorisation administrative d'accès à des sites classés.

Le « New Deal mobile » est donc vraiment entré en phase industrielle. Nous avons un partenariat exemplaire avec les collectivités et les parlementaires.

Nous avons continué à déployer durant le confinement, malgré quelques problèmes d'approvisionnement en pylônes. C'est pour nous, Fédération et opérateurs, un enjeu extrêmement important.

Vous nous avez interrogés sur notre conception de la souveraineté numérique pour notre secteur. Sans rentrer dans les détails que mes collègues compléteront, nous pensons que l'effet du numérique sur la souveraineté est très important puisque ce domaine fait émerger un certain nombre de géants économiques dont la puissance économique et financière peut rivaliser avec certains États. Ces géants conquièrent des marchés en se jouant des régulations et n'ont pas du tout les mêmes régulations ni les mêmes obligations que les opérateurs. Nous le regrettons mais, tout en partant de ce constat, je souhaite être un peu plus optimiste.

Pour nous, la souveraineté numérique s'appréhende d'abord à l'aune de la qualité des réseaux fixes et mobiles. Les infrastructures numériques en France sont résilientes comme nous l'avons prouvé pendant le confinement, innovantes et performantes. Elles sont même extrêmement performantes et pérennes. Lorsque le plan France Très Haut Débit a été initié en 2013, beaucoup de pays européens nous regardaient bizarrement mais ce réseau nous est aujourd'hui envié. L'Allemagne vient de mettre 7 milliards d'euros pour déployer un certain nombre d'infrastructures parce qu'ils ne sont pas dans une aussi bonne situation que la nôtre. Nous faisons vraiment la promotion de ce réseau et la souveraineté numérique passe d'abord par un réseau important.

L'Europe a selon nous toutes les qualités pour créer ses propres champions du numérique. Nous avons des réseaux de qualité, une longue tradition de recherche scientifique, d'excellents ingénieurs scientifiques même si nous pouvons regretter que certains s'expatrient hors d'Europe. Nous disposons aussi d'un environnement extrêmement dynamique de start-up. Nous pensons donc que l'Europe est le lieu où doit pouvoir se déployer dans les prochaines années tout l'avenir de cette souveraineté, en passant par l'intelligence artificielle, la cybersécurité, la sécurité des réseaux. Nous avons un socle très solide sur lequel nous pouvons capitaliser.

Les opérateurs travaillent avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur la sécurité des réseaux, notamment de la 5G. C'est leur métier

depuis plus de vingt ans. Les opérateurs ont toujours respecté les préconisations de sécurité des réseaux pour la 2G, pour la 3G, pour la 4G et feront de même pour la 5G. Nous avons donc des réseaux extrêmement sûrs.

Sur la 5G, nous pouvons regretter les conditions un peu précipitées dans lesquelles la loi sur la sécurité des réseaux a été introduite à l'été 2019 avec, selon nous, un manque d'anticipation et de concertation avec les acteurs télécoms que nous sommes. Nous avions déjà souligné à l'époque deux points : le caractère rétroactif de cette loi et le délai de traitement des autorisations. Même en tenant compte de la parenthèse covid, force est de constater que les autorisations délivrées par l'ANSSI l'ont été de manière tardive.

Je souligne un dernier point qui ne fait pas partie du spectre consensuel de la Fédération : ni la loi ni le décret n'ont prévu un dédommagement pour les opérateurs qui devraient éventuellement démonter des infrastructures.

Nous avions signalé tous ces points et nous regrettons le manque d'anticipation. Ceci étant dit, nous respectons bien évidemment toutes ces règles et nous sommes très attachés à la sécurité des réseaux. Créer des réseaux le plus innovants possible est d'ailleurs notre métier.

La 5G provoquera une virtualisation des réseaux ; il n'existera plus de véritable connexion, tout sera en lien. Cela crée un véritable enjeu au niveau européen pour être capables d'une véritable harmonisation entre tous les États membres de l'Union, même si je sais que ce n'est pas facile en particulier sur le plan fiscal. Nous nous réjouissons de l'initiative récente de la Commission européenne qui veut travailler à un outil pour définir des standards uniformes.

Nous saluons l'initiative prise en 2019 par la France de créer une taxe sur les services numériques. Nous la portons depuis plusieurs années mais nous pensons que cette décision devrait être prise au moins à l'échelon européen, dans l'idéal au niveau de l'Organisation de coopération et de développement économiques (OCDE). Les négociations internationales n'avancent pas. Elles sont embourbées du fait d'intérêts qui nous dépassent largement entre la Chine et les États-Unis.

Cette taxe existe ; cela va dans le bon sens mais c'est une goutte d'eau par rapport aux géants du web (GAFAM). Au-delà de la fiscalité sectorielle qui pèse sur les télécoms et que les GAFAM ne supportent pas, les GAFAM paient vingt-cinq fois moins d'impôt sur les sociétés que les opérateurs de la Fédération. Ce premier pas doit donc être confirmé même si c'est extrêmement compliqué et si la question va bien au-delà de notre petit marché européen.

Nous saluons également les initiatives lancées au niveau européen sur le droit de la concurrence, notamment pour créer un cadre de régulation qui s'applique aux géants du Net. Notre secteur est extrêmement régulé, par l'ARCEP au niveau de déploiements, par le Conseil supérieur de l'audiovisuel (CSA) au niveau audiovisuel qui est un domaine dans lequel certains acteurs sont très présents. Nous plaidons pour une régulation qui s'applique à l'ensemble des nouveaux entrants et des grands acteurs. Il s'agit de faire émerger des nouveaux services, des start-up, mais que nous soyons tous à armes égales. L'ensemble doit être conçu au bénéfice du consommateur.

Nous connaissons les grands gagnants de la crise sanitaire. Il suffit de regarder la progression de Netflix et d'autres applications. Ils sortent largement vainqueurs. Ils utilisent des réseaux performants et résilients sans participer pour un centime à l'aménagement numérique du territoire.

Mme Ombeline Bartin, responsable des relations institutionnelles d'Iliad / Free. Je représente le groupe Iliad, maison-mère de Free mobile mais aussi l'opérateur fixe Free qui existe en France depuis vingt ans. Nous sommes aussi présents en Europe, en Italie et nous avons acheté un opérateur mobile en Pologne. Nous travaillons donc à la construction d'acteurs européens solides qui permettront certainement de garantir une meilleure souveraineté européenne.

Même si nous ne sommes pas membres de la FFT, nous sommes alignés en tout point sur les éléments que vient d'énoncer Oliver Riffard sur la souveraineté numérique. Je souligne que nous avons en France la chance d'avoir quatre opérateurs français solides, compétitifs et indépendants. Ces acteurs ont tous un actionnariat majoritairement français avec des actionnaires solides et investissent massivement dans des infrastructures déployées sur tout le territoire à grande vitesse et même à un rythme inédit en Europe. Ces infrastructures offrent une sécurité importante, d'une part en termes de maillage territorial puisque nous couvrons aujourd'hui la majorité des zones rurales et que nous en couvrirons la totalité assez rapidement, d'autre part en termes de continuité de service puisque les opérateurs conçoivent leurs réseaux pour parer à toute interruption de service avec beaucoup de redondance des équipements et des opérateurs en présence. Les réseaux sont construits de telle sorte que l'ensemble du réseau ne tombe pas si une attaque a lieu sur une partie du territoire et que d'autres parties du réseau puissent prendre le relais.

Pour nous, la souveraineté numérique consiste à avoir des opérateurs solides, des infrastructures fortement déployées, redondantes, accessibles sur l'entièreté du territoire et à offrir aux opérateurs la maîtrise de leurs équipements, de leur réseau. Ce dernier point passe par la gestion de la sous-traitance et de la maintenance de leur réseau mais aussi par le choix des équipements que les opérateurs exploitent.

Nous n'avons aucun doute sur l'utilité de la loi 5G. Il appartient bien évidemment à l'État de surveiller quels sont les équipements autorisés sur nos réseaux. Néanmoins, la mise en œuvre de cette loi soulève beaucoup de questions. Nous nous interrogeons aujourd'hui en termes de sécurité publique. Certains opérateurs sont autorisés à exploiter des équipements sur certaines zones du territoire tandis que d'autres opérateurs ne le sont pas pour des motifs de sécurité publique. Nous nous demandons donc pourquoi ces équipements seraient dangereux en termes de sécurité publique pour certains mais pas pour d'autres. Cette loi conduit à un résultat un peu fragile car elle semble inéquitable et est contestée par une partie des opérateurs.

M. le président Jean-Luc Warsmann. Pourriez-vous détailler ce que vous venez de dire ?

Mme Ombeline Bartin, responsable des relations institutionnelles d'Iliad / Free. La loi visant à autoriser de façon préalable l'exploitation des équipements 5G sur les réseaux mobiles prévoit un régime d'autorisation de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) qui délivre ces autorisations sur des motifs de sécurité nationale, de défense publique. Elle prend en compte les degrés de déploiement des réseaux et les conditions d'exploitation de ces équipements par les opérateurs.

Comme l'a souligné M. Riffard, nous avons mis beaucoup de temps à obtenir ces autorisations. Nous avons obtenu lors d'une première vague les autorisations expresses d'accord mais pas les refus. Il a fallu en faire la demande pour obtenir les refus et les motifs indiqués sont très sommaires.

Free mobile exploite des équipements Huawei sur une petite partie du réseau correspondant aux zones rurales dans lesquelles nous déployons des sites pour zone blanche

ou répondant aux besoins du dispositif de couverture prioritaire. Pour ces zones qui ne sont pas à forte densité, dans lesquelles il n'existe *a priori* pas d'infrastructure critique, l'autorisation d'exploiter en 5G avec du matériel Huawei ne nous a pas été délivrée. Nous nous interrogeons sur la façon dont est appliquée cette loi puisque, pour des zones semblables, Huawei a été autorisé pour d'autres opérateurs.

Notre question est donc de savoir s'il existe des motifs de sécurité publique qui puissent être valables pour certains opérateurs mais pas pour d'autres et comment le justifier. Plus globalement, la mise en œuvre de cette loi est assez contestée. D'autres opérateurs ont déposé un recours devant le Conseil d'État.

Pour nous, finalement, l'important pour la souveraineté numérique est d'avoir des opérateurs solides, des infrastructures denses, redondantes et que les opérateurs soient au cœur du dispositif de lutte contre les cyberattaques et les cybercrimes, en interaction constante avec l'ANSSI et les autorités légales pour renforcer la sécurité de nos réseaux pour nos clients particuliers et professionnels.

Mme Claire Perset, secrétaire générale adjointe de SFR. Je suis évidemment en phase avec ce qui vient d'être dit par Ombeline Bartin et Olivier Riffard. Je pense que la solidité des opérateurs et des réseaux est le point principal.

Le confinement a bien montré que nos réseaux sont extrêmement solides. Cette crise a été un véritable test puisque la France entière télétravaillait, tandis que les élèves suivaient leurs cours en ligne. Tout le monde était plus que jamais connecté. Si certains avaient des doutes sur la solidité de nos réseaux, je pense qu'ils n'en ont plus désormais.

Nous investissons plusieurs milliards d'euros chaque année dans les réseaux. C'est un élément clé et c'est aussi un élément de distorsion par rapport aux GAFAM. Nous investissons et nous déployons des infrastructures que les GAFAM utilisent sans participer aux investissements.

Je rappelle que les opérateurs réussissent à déployer le très haut débit dans des délais record, même si nos concitoyens sont impatients et trouvent que nous n'allons pas assez vite. Le déploiement de l'électricité dans la France entière a demandé quasiment un siècle tandis que le déploiement du très haut débit aura demandé vingt ans.

S'agissant de la sécurité et de la question de Huawei, je redis comme mes collègues que nous travaillons au quotidien avec l'ANSSI pour la sécurité de nos réseaux 3G, 4G et 5G. Nous respectons évidemment les impératifs de sécurité nationale et la législation en vigueur. Pour autant, les décisions d'interdiction d'utilisation de Huawei ont pour nous des conséquences très importantes. Nous allons en effet devoir déconstruire puis reconstruire une part substantielle de nos réseaux. Sur les plans économique et financier, les conséquences en sont très lourdes puisque ce sont des investissements colossaux que nous n'avions pas prévus. Nous demandons donc une compensation comme c'est le cas aux États-Unis où un fonds de compensation a été créé pour les opérateurs concernés.

Je rappelle aussi que tous nos *data centers* sont situés en France, ce qui est une garantie importante pour la sécurité des données.

J'insiste sur la distorsion de concurrence avec les GAFAM, que ce soit en termes d'investissements ou de fiscalité, même si nous allons dans le bon sens avec la taxe qui a été votée. C'est un premier pas mais ce n'est encore qu'une goutte par rapport à ce que les opérateurs pourraient attendre pour un véritable rééquilibrage de la concurrence.

M. Anthony Colombani, directeur corporate de Bouygues Telecom. Je souscris à ce qui a été dit par les précédents intervenants.

J'étais, voici des années, professeur de géographie et, à l'époque, nous travaillions beaucoup sur le général Lucien Poirier, un des pères de la dissuasion nucléaire française. Lucien Poirier définissait la souveraineté comme la capacité de décider seul. Je pense que c'est au fond bien ce dont nous parlons aujourd'hui. L'État est souverain lorsqu'il peut décider seul ou avec des acteurs de confiance.

Je définis donc la souveraineté numérique comme reposant sur trois piliers. Le premier est de disposer d'opérateurs solides, bien capitalisés, qui ne sont pas à la main de fonds de pension étrangers. Je crois que c'est le cas des opérateurs français. Ils investissent, ne se lancent pas dans des aventures mais montrent, par leur sérieux, qu'ils sont présents depuis plusieurs décennies sur le territoire et que nous n'avons aucune inquiétude à avoir à leur sujet.

Le deuxième pilier est de disposer de réseaux performants. Nous avons vu pendant la crise qu'un certain nombre de services étaient assurés par ces réseaux et qu'il était absolument nécessaire qu'ils soient performants, redondants, sécurisés, avec de bons niveaux d'alerte positionnés aux bons endroits en cas d'attaque, en cas de réseau qui tombe… Je ne crois pas qu'une entreprise française ait pu avoir des difficultés opérationnelles fortes ou être mise en danger par des réseaux de mauvaise qualité même si nous pouvons évidemment toujours progresser. Ce n'est pas le cas dans tous les pays. Aux États-Unis, l'état des réseaux en cuivre et des réseaux optiques a parfois mis en danger l'activité économique.

Le troisième pilier est d'avoir des opérateurs qui travaillent en confiance avec les autorités. Nous avons évoqué l'ANSSI et nous pouvons évoquer aussi nos activités dites « d'obligation légale », c'est-à-dire les activités par lesquelles nous avons un dialogue constant avec les autorités pour mener toutes les actions nécessaires à la force publique. Nous communiquons peu sur ce point mais nous en sommes très fiers car c'est un élément très fort de la souveraineté.

J'attire toutefois votre attention sur le fait que les mutations technologiques ont tendance à cacher de plus en plus le trafic aux opérateurs. Une grande partie du trafic voix et data est aujourd'hui cryptée ; ce trafic passe par des systèmes de DNS et échappe aux opérateurs. Ceci constitue un vrai sujet de souveraineté puisque, pour obtenir ces informations, il ne faut pas aller taper à la porte des opérateurs qui ont tous leurs sièges sociaux dans un rayon de quelques kilomètres autour de l'Assemblée nationale mais à la porte d'intermédiaires techniques ou d'acteurs étrangers qui ne répondent pas toujours avec la célérité nécessaire.

Sur la 5G, nous ne contestons pas le principe de la loi. Que l'État se mêle de la sécurité de ces infrastructures n'est évidemment pas contestable. Nous respectons cette loi à la lettre, dans les délais prescrits et avec toute la célérité nécessaire comme il convient pour un acteur responsable. Néanmoins, cette loi pose des problèmes opérationnels évoqués par Ombeline Bartin pour la question des délais, par Claire Perset pour la question financière. Nous devons aujourd'hui démonter une grande partie de nos infrastructures. Cela a un coût financier et cela a aussi un coût pour les clients parce que ces opérations de *swap*, c'est-à-dire de changement d'équipements, génèrent des difficultés ponctuelles qui peuvent être compliquées à gérer. Je tiens à être bien clair : nous ne contestons pas le principe de la loi mais une partie de sa mise en œuvre.

La 5G est un véritable sujet de souveraineté. La 5G est le réseau du futur. Elle sera très utilisée par nos entreprises et sera un élément très fort de compétitivité. Ce sera un élément clé dans la concurrence internationale. Nous voyons que la 5G se déploiera avec un certain nombre de difficultés. Dans l'opinion publique et chez certains élus, nous constatons une

véritable méfiance, parfois même une vraie défiance, ce qui a conduit certains d'entre eux à prendre des moratoires qui créent évidemment des difficultés pour nous. Il ne faudrait pas que cette opposition larvée à la 5G, parfois violente puisqu'une quarantaine d'antennes ont brûlé en France, nous fasse prendre du retard. C'est un point extrêmement important. Nous comptons vraiment sur les parlementaires, les pouvoirs publics, les élus et les différentes autorités pour faire de la pédagogie et vaincre un peu ces résistances. Les opérateurs ne pourront pas le faire seuls. Nous avons certes le droit pour nous mais ces conditions sont insupportables pour nous et ne correspondent évidemment pas à nos valeurs.

En ce qui concerne les aspects économiques, Olivier Riffard vous transmettra l'ensemble des chiffres sur la fiscalité. Il me semble qu'il faut revenir aux bases. Nous savons depuis la construction de l'État moderne, au moins depuis Louis XIII, que la souveraineté est d'abord la souveraineté fiscale, la capacité à faire payer l'impôt aux gens qui gagnent de l'argent. Aujourd'hui, la différenciation fiscale entre nous et d'autres acteurs qui sont parfois nos concurrents directs est abyssale. Depuis des années nous sont promis des taxes, des renouvellements, un environnement équitable, des dispositions qui permettent de tout mettre à niveau mais c'est très lent.

Ce n'est d'ailleurs pas vrai uniquement dans le domaine fiscal mais aussi dans le domaine réglementaire. Un exemple très ponctuel mais très parlant est celui de l'impact environnemental du numérique. Dans le cadre de la loi sur l'économie circulaire votée récemment, il a été imposé aux opérateurs de communiquer sur les émissions de gaz à effet de serre liés aux usages numériques. À partir du 1er janvier 2022, nous devrons communiquer à chacun de nos clients le fait que sa consommation de 2, 3, 5 ou 10 gigas de données fixes ou mobiles a occasionné l'émission de tant de kilogrammes de CO_2. Il n'est passé par l'esprit de personne d'imposer cette obligation aux GAFAM. Il nous a été demandé de le faire, nous le faisons, nous nous mettons en ordre de marche, cela nous prend du temps et de l'énergie mais personne n'a pensé que cette obligation pourrait aussi être imposée à Google et à Amazon. Lors du téléchargement d'un film ou de la commande d'un colis, il ne serait pourtant pas complètement idiot de donner l'équivalent en émission de gaz à effet de serre. Nous aurions donc vraiment besoin de cet environnement équitable, ce *level playing field*. Les discours politiques laissent à penser qu'il est en cours de mise en œuvre mais, malheureusement, sur le terrain, nous vérifions que ce n'est pas le cas. Il est parfois facile de taper sur les opérateurs qui sont à portée de main tout en oubliant qu'il serait bon que le bras du législateur aille plus loin.

M. Philippe Latombe, rapporteur. L'Europe a la volonté de mettre un peu d'ordre dans les réseaux sociaux et de réguler les réseaux, notamment en imposant des retraits de contenus. Je pense à la proposition de loi « Avia » qui est pour partie reprise, au moins dans son esprit, dans la réglementation européenne en préparation. Ces obligations incombent aux opérateurs. Nous avons eu parallèlement un appel à la Cour de justice de l'Union voici quelques mois sur la conservation des métadonnées.

Comment voyez-vous plus généralement le rapport entre la réglementation européenne et la réglementation nationale, vous concernant ? Selon vous, quel serait le meilleur champ pour un certain nombre de sujets ? Par exemple, sur la sécurité des réseaux, le niveau français, national est-il le plus pertinent ? Sur la partie des données, le niveau européen est-il mieux ? Comment voyez-vous l'architecture entre la réglementation européenne et la loi nationale ?

M. le président Jean-Luc Warsmann. Vous êtes plusieurs à avoir dit du bien du réseau français. En quoi le réseau français est-il plus sécurisé que, par exemple, le réseau allemand ? Pouvez-vous décrire quelles sont les sécurités que vous estimez suffisantes ou supérieures dans le réseau français ?

M. Olivier Riffard, directeur des affaires publiques de la FFT. Depuis plusieurs années, les opérateurs ont, d'après la loi, l'obligation de retirer extrêmement rapidement, c'est-à-dire en quelques heures, les contenus pédopornographiques et terroristes. Dans ces deux cas, et c'est la seule exception, nous ne passons pas par la case « juge ». Le système marche et nous le faisons très rapidement. L'actualité récente fait que nous avons enfin mis sur le devant de la scène la plateforme de signalement Pharos, à laquelle tout remonte. Il faut savoir que la Fédération française des télécoms fait office de filtre : tout ce qui est remonté sur les contenus pédopornographiques et terroristes passe par un premier filtre technique de la Fédération pour voir si la caractérisation des faits sera ensuite exploitable par la plateforme Pharos. Nous demandons depuis des années une véritable prise de conscience, que nous ayons des effectifs formés et beaucoup plus nombreux pour Pharos, que soit créé le fameux parquet numérique. Toutes ces nouvelles infractions, ces nouvelles atteintes à la vie privée et autres ne sont aujourd'hui pas traitées à un niveau suffisant par les tribunaux.

Chacun sait où trouver les opérateurs, les fournisseurs d'accès internet que nous sommes. Le réflexe est de nous demander de couper les contenus, ce qui ne nous pose aucun problème puisque nous respectons comme d'habitude scrupuleusement les lois. Toutefois, il existe de multiples intermédiaires techniques, des hébergeurs et des moteurs de recherche qui échappent de fait à toutes ces obligations.

Nous pensons qu'il faudrait en premier lieu avoir une harmonisation européenne comme nous l'avions dit pour la proposition de loi « Avia ». Il semble qu'une prise de conscience européenne ait lieu. L'objectif de cette proposition de loi était d'être précurseur mais nous avons bien vu que, juridiquement et au niveau de la mise en œuvre, la question était plus compliquée. Le problème s'est posé de la même façon pour tous les débats liés à l'empreinte du numérique, à l'économie circulaire, à la réparabilité des téléphones portables. Nous nous apercevons aujourd'hui que ces problèmes devraient plutôt être traités au niveau européen.

Il faut que tous les acteurs de la chaîne de valeurs soient appréhendés. S'agissant des contenus et de la sécurité, les hébergeurs et les moteurs de recherche sont donc concernés. C'est à eux qu'il faut demander de supprimer des contenus puisque, en vertu des principes de la neutralité du Net, nous n'avons pas vocation à regarder ce qui passe dans nos réseaux et nous en avons même l'interdiction. Si nous regardons ce qui passe dans nos tuyaux, nous sommes en infraction. Aussi, lorsque le juge nous demande de couper telle ou telle page sur Facebook, nous ne sommes pas capables de faire une coupe chirurgicale contrairement aux autres acteurs intermédiaires et nous coupons l'accès à Facebook de tous nos clients, ce qui pose des questions de proportionnalité par rapport à l'atteinte.

Lorsque je parlais de l'Allemagne, je ne pensais pas à la sécurité des réseaux sur laquelle je n'ai pas de données mais à la qualité de nos réseaux. Il faut savoir que l'Allemagne a fait le choix depuis une dizaine d'année de monter en débit sur le très haut débit et que, aujourd'hui, le système explose complètement. Ils n'ont plus suffisamment de capacités et réfléchissent maintenant à la fibre. Sur le mobile, l'Angleterre et l'Allemagne ne couvrent pas les zones blanches et investissent des milliards en s'inspirant du « New Deal mobile ». Je voulais dire que la qualité de connexion de nos réseaux est extrêmement bonne et nous nous en apercevons puisque, que ce soit de la part des pouvoirs publics ou des élus, nous sommes en train de glisser de « je n'ai pas de connexion, cela ne marche pas » à des questions liées à l'inclusion numérique, à l'empreinte du numérique, au fait que Nantes par exemple ne veut pas d'antenne 5G en jugeant que la 4G suffit.

Nous pensons que, sur les questions de fiscalité et de régulation des contenus, une approche européenne coordonnée est vraiment nécessaire. La principale difficulté provient du

fait que nous avons quatre opérateurs en France, plus de quatre-vingts en Europe et une trentaine de régulations différentes, ce qui complique beaucoup l'harmonisation. Nous pensons malgré tout que tout ce qui concerne la souveraineté et l'émergence de champions du numérique passera par une approche coordonnée et harmonisée.

M. le président Jean-Luc Warsmann. Je suis élu de la région Grand Est dans laquelle, dans quelques mois, tout le monde sera desservi en très haut débit (THD), même dans les plus petits villages.

M. Anthony Colombani, directeur corporate de Bouygues Telecom. Le niveau européen est toujours meilleur car il apporte une sécurité juridique et une harmonisation. Toutefois, rien n'empêche un État de prendre des dispositions différentes sur les sujets qu'il juge sensibles, voire relevant de sa souveraineté, à condition que ces dispositions soient prises proprement. La loi « Avia » était une initiative parfaitement justifiée par le niveau de violence, voire de barbarie, qui règne sur certains réseaux mais ce n'était manifestement pas la bonne manière de procéder puisque le texte a été taillé en pièces par le Conseil constitutionnel.

Ce sujet précis du retrait des contenus haineux relève d'ailleurs d'une forme de souveraineté. Cela ne concerne pas que les contenus haineux mais aussi la possible manipulation d'élections ou les *fake news* qui sont un sujet de souveraineté démocratique. Il faut rappeler que l'obligation de retrait des contenus n'incombe pas aux opérateurs au sens des fournisseurs d'accès internet mais bien aux plateformes puisque, en vertu de notre statut de tuyaux, nous ne regardons pas ce qui circule. Nous ne coupons pas l'accès aux contenus, sauf si le juge nous le demande et dans des conditions extrêmement précises. Il s'agit surtout d'une question de moyens en réalité. Aujourd'hui, lorsque nous voulons retirer un contenu, condamner un fauteur de troubles, quelqu'un qui émet des messages de haine, de harcèlement, des appels au viol ou autres qui sont parfois très lourdement condamnés, le problème est plutôt celui des moyens accordés à la justice que l'architecture législative et réglementaire.

M. Philippe Latombe, rapporteur. Imaginons que vous êtes à la fois législateur et exécutant, que vous possédez une baguette magique et avez la possibilité de faire ce que vous voulez. Comment modifiez-vous la fiscalité ? Vous avez dit avoir l'impression – vérifiée par les chiffres – d'être fiscalement largement assujettis alors que les GAFAM ne le sont pas. Comment verriez-vous une modification fiscale, à quel niveau et surtout de quelle façon ?

Vous êtes physiquement présents sur le territoire national et en Europe puisque vous avez des réseaux tandis que les GAFAM ne sont pas forcément présents de la même façon. Vous êtes des tuyaux et eux fournissent du contenu. Comment voyez-vous l'évolution de la fiscalité pour les GAFAM ?

M. Olivier Riffard, directeur des affaires publiques de la FFT. Sans baguette magique et sans me placer par rapport aux GAFAM, je proposerais de supprimer la fiscalité spécifique sectorielle qui s'applique uniquement au secteur des télécoms et est unique au monde. En effet, une fois les 1,3 milliard d'euros d'impôts sur les sociétés payés par les trois opérateurs que je représente, les opérateurs paient, en plus des 10 milliards d'euros qu'ils investissent, encore 1,3 milliard d'euros de fiscalité spécifique qui se décompose en trois taxes.

La première est la taxe sur les opérateurs de communication électronique (TOCE) créée en 2009 suite à la suppression de la publicité après 20 heures sur France Télévisions. Cette taxe, qui n'est plus affectée à France Télévisions depuis 2019 suite à une décision du Parlement, a rapporté plus de 2,6 milliards d'euros au budget de l'État. Nous souhaiterions que cette taxe soit supprimée et affectée plutôt aux opérateurs pour que nous puissions déployer encore plus de réseaux.

Les opérateurs financent également le Centre national du cinéma et de l'image animée (CNC). C'est très bien mais nous ne voyons pas pourquoi les opérateurs privés qui, par ailleurs, sont aussi éditeurs de contenus et ont même des plateformes auraient à financer la culture. Nous souhaitons donc aussi la suppression de cette taxe.

La troisième, encore plus injuste, est l'imposition forfaitaire des entreprises de réseaux (IFER), créée pour remplacer la taxe professionnelle. Plus nous déployons d'antennes mobiles, plus nous sommes taxés. Cette taxe représente 1,6 milliard d'euros depuis sa création en 2011.

La suppression de ces taxes permettrait que les opérateurs puissent plus facilement assurer l'investissement maximum avec les prix les plus bas d'Europe par comparaison aux autres secteurs régulés que sont l'électricité et le gaz.

M. Anthony Colombani, directeur corporate de Bouygues Telecom. J'appliquerais d'abord les recommandations de l'OCDE. Des milliers de pages de rapports ont été écrites pour décrire finement les mécanismes utilisés pour faire de l'évasion fiscale – *Dutch Sandwich*, *Double Irish* qui ressemblent à des plats de fast-food un peu gras – et je pense que je taxerais le chiffre d'affaires dans le pays donné. Nous avons un géant du commerce en ligne, un géant des contenus ; je regarderais le chiffre d'affaires, je le taxerais et je mettrais fin aux mécanismes subtils par lesquels le rachat de la licence de marque à la maison-mère permet de faire artificiellement baisser son revenu sur l'année. Je ne suis pas fiscaliste mais géographe ; cela me semble être une manière de faire.

Mme Claire Perset, secrétaire générale adjointe de SFR. Il est important de rappeler que l'IFER est un impôt exponentiel puisque plus nous déployons, plus nous sommes taxés. Cet impôt a un côté complètement schizophrène : on nous demande de déployer toujours plus mais que nous sommes alors plus taxés. Je sais que les parlementaires en ont bien conscience. Plusieurs députés dont Mme de La Raudière nous ont soutenus sur ce sujet. Nous menons ce combat depuis un moment, nous ne nous sentons pas seuls et nous espérons des changements cette année puisqu'un rapport de l'Inspection générale des finances (IGF) sera rendu.

Mme Ombeline Bartin, responsable des relations institutionnelles d'Iliad / Free. Je souscris totalement aux propositions faites. Je rajoute que les opérateurs français investissent 10 milliards par an pour le déploiement de ces réseaux très haut débit fixe et mobile. Or, nous constatons que ces réseaux sont très majoritairement occupés par les contenus des grands acteurs américains. Nous avons déjà essayé de porter ce sujet de savoir comment ces acteurs américains, qui occupent 75 % de notre bande passante, pourraient également participer à l'effort de construction du chantier en cours, sur la fibre optique et la densification des réseaux mobiles. Nous nous sommes toujours heurtés, sous couvert de la neutralité d'internet, à l'impossibilité de faire contribuer ces acteurs à la construction et la maintenance de nos réseaux. Nous le regrettons d'autant plus que nous sommes convaincus que la neutralité de l'internet est davantage destinée à protéger les petits acteurs pour qu'ils puissent diffuser leurs contenus librement, dans des conditions non discriminatoires, plutôt qu'à protéger ces grands acteurs américains.

Mme Laure de La Raudière. Corinne Erhel et moi-même avions imaginé pousser au niveau européen l'idée d'avoir une terminaison d'appel data, ce qui permettrait une régulation nouvelle plutôt que de revenir sur la neutralité d'internet. Nous n'avons à mon avis pas intérêt à toucher à la neutralité d'internet mais peut-être plutôt intérêt à porter le concept de neutralité sur d'autres sujets comme les plateformes et les terminaux. Pour favoriser l'innovation, l'économie, la liberté d'expression, nous ne devons pas toucher à la neutralité des réseaux.

J'aimerais avoir votre avis sur ce que nous avions imaginé comme terminaison d'appel data, c'est-à-dire que les injecteurs de trafic paient une partie de l'ensemble du fonctionnement du réseau, pas seulement leur raccordement au réseau. Qu'en pensez-vous ?

M. Anthony Colombani, directeur corporate de Bouygues Telecom. Nous y souscrivions à l'époque et nous y souscrivons toujours. Au-delà d'un certain niveau d'asymétrie de trafic, cela ne paraît pas complètement idiot de faire payer une terminaison d'appel data. C'est une des manières de faire.

Nous nous inquiétons aussi au plan environnemental. Si les GAFAM occupent 75 % de nos réseaux aux heures de pointe, elles occasionnent aussi 75 % de la consommation énergétique et des émissions de gaz à effet de serre. Il faut aussi répondre à cet enjeu environnemental. Enfin, ce n'est certes pas vraiment 75 % mais c'est une partie du problème et il faut mettre fin à certaines pratiques, peut-être avant la mise en œuvre de la terminaison d'appel data qui prendra un peu de temps car il est très difficile de mettre tout le monde d'accord.

Il faut interdire un certain nombre de pratiques, telles que l'enchaînement sans fin de vidéos, le fait de pousser du flux 8K sur des écrans 480p. Beaucoup de solutions très pratiques et très concrètes existent pour faire baisser la pression sur les réseaux et contribuer à une modération de la consommation énergétique.

La terminaison d'appel data reste le point d'arrivée le plus intéressant mais il faudra mettre d'accord les pays européens entre eux et avec le pays qui est le berceau de tous ces géants. Ce sera sans doute compliqué.

M. Olivier Riffard, directeur des affaires publiques de la FFT. Nous pensons aussi que les États européens peuvent mettre un peu plus de pression sur ces acteurs, mettre une véritable pression politique. Par exemple, au début du confinement, nous étions très inquiets quant au fait que les réseaux tiendraient car ces acteurs envoient – c'est leur modèle de fonctionnement – des qualités de service et des niveaux de définition extrêmement élevés. À force de le leur demander, ils ont finalement accepté de décaler de quelques jours la sortie de Disney+, qui n'existait pas voici quelques mois et est maintenant juste en dessous de Netflix dans les plateformes de vidéo. Netflix a 63 % de parts de marché et Disney+ en a 30 %. Ils ont aussi accepté de diminuer la qualité de leurs vidéos. À ma connaissance, nous n'avons pas eu de manifestation dans la rue d'usagers qui ne pouvaient plus utiliser Netflix ou d'enfants qui recevaient des vidéos en 4K sur leurs terminaux.

Le secteur est parfois un peu agacé par la façon dont ces acteurs font leur lobbying. Nous sommes transparents, nous participons à l'aménagement du territoire, tandis qu'ils ont une autre façon de procéder. C'est agaçant de voir tel ou tel membre du Gouvernement s'afficher avec tel ou tel géant de l'internet tandis que les opérateurs ne sont pas mis au même niveau alors qu'ils pratiquent aussi ces sujets.

Sur la régulation des contenus, c'est trop facile lorsque Facebook ou Twitter disent qu'ils s'en occupent, qu'ils ont mis les moyens humains et financiers et se réguleront eux-mêmes. Si nous affirmions que nous déploierons la 5G en regardant nous-mêmes la sécurité des équipements, cela ne passerait pas. Ce « deux poids, deux mesures » est agaçant, au-delà de la fiscalité, même si nous ne remettons pas en cause l'innovation et l'apport de ces géants. Nous ne voulons pas nous dresser les uns contre les autres mais il faut que nous soyons à armes égales.

M. Philippe Latombe, rapporteur. Je vous remercie et j'ai pris bonne note en particulier de la question des flux qui est peut-être un aspect très simple à mettre en œuvre.

Audition, ouverte à la presse, de représentants des sociétés de télécommunications Ericsson, Huawei et Nokia : M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson, M. Minggang Zhang, directeur général adjoint, Mme Linda Han, déléguée générale et M. Jean-Christophe Aubry, responsable des affaires publiques, de Huawei France, M. Marc Charrière, directeur des affaires publiques de Nokia
(26 novembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je suis très heureux d'accueillir les représentants des trois principaux équipementiers du secteur des communications électroniques, Ericsson, Huawei et Nokia. Je salue donc M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson. Pour Huawei sont présents M. Jean-Christophe Aubry, responsable des affaires publiques, Mme Linda Han, déléguée générale de Huawei France et M. Minggang Zhang, directeur général adjoint de Huawei France. Nokia est représenté par M. Marc Charrière, directeur des affaires publiques.

Cette audition s'inscrit dans le cadre des réflexions que notre mission mène sur la souveraineté numérique.

M. Philippe Latombe, rapporteur. Cette audition est une prise de contact utile pour aborder le sujet de la souveraineté numérique de façon globale.

Je voudrais d'abord vous interroger sur le sens que revêt pour vous la notion de souveraineté numérique au sein de votre secteur d'activité. Ce concept, parfois rapproché de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et de ne pas subir les contraintes imposées par certains acteurs publics ou privés, qu'il s'agisse d'États ou des géants du web (GAFAM). Je souhaite avoir votre point de vue sur cette préoccupation croissante des États, particulièrement en France.

De façon plus générale, nous souhaitons vous entendre sur les grandes caractéristiques de votre secteur d'activité et sur l'impact de la crise de la covid-19 sur vos activités en France, en Europe et dans le monde. Nous nous interrogeons en effet sur les conséquences de cette crise pour les acteurs qui dépendent de vos produits, au premier rang desquels l'ensemble des entreprises et opérateurs qui déploient des réseaux de communication électronique.

Je souhaite aussi aborder avec vous le sujet de la 5G dont les enchères sont achevées pour la bande des 3,5 gigahertz. Des offres commerciales ont été lancées. Dans ce contexte, alors qu'un régime d'autorisation très spécifique a été mis en place par le législateur, nous aimerions vous entendre sur la sécurité des équipements installés en France, aussi bien vis-à-vis des cyberattaques que des pratiques comme l'espionnage.

Nous aimerions également aborder avec vous les enjeux de la bataille normative qui s'engage entre la Chine, l'Europe et les États-Unis.

Enfin, cette mission s'intéresse aux aspects économiques de la souveraineté numérique, aussi bien la fiscalité que la concurrence. Nous sommes intéressés par vos réflexions sur ces deux points.

M. Marc Charrière, directeur des affaires publiques de Nokia. Il me semble important de redire que la 5G n'est pas uniquement l'accès mobile, pas uniquement l'évolution de la 3G et de la 4G pour le grand public même si c'est ce qui est mis en place actuellement avec l'attribution des fréquences de la bande des 3,5 gigahertz. La 5G va bien au-delà et constitue un grand enjeu pour les « marchés verticaux », c'est-à-dire tous les autres secteurs industriels. Ils pourront bénéficier de cette technologie aussi bien pour la voiture autonome que l'industrie 4.0 en passant par la gestion des machines-outils.

Bien gérer ce passage à la 5G et la virtualisation des réseaux est très important pour l'évolution de l'économie et donc pour les États de façon générale. Cette virtualisation consiste en la mise en place de plateformes logicielles réservées aux réseaux. Il s'agit de créer des réseaux suffisamment versatiles, capables de s'adapter en temps réel pour fournir toutes les applications dont les secteurs industriels auront besoin.

Il faut noter que les réseaux ne sont plus constitués de boîtes contenant du « *hardware* » et des logiciels que nous connectons puis que nous gérons. Nous sommes carrément en train de déplacer le logiciel qui se trouve dans les boîtes sur des plateformes logicielles situées entre l'infrastructure réseau des boîtes et les applicatifs auxquels nous sommes habitués. Actuellement, les plateformes hébergent des applicatifs, pour vous et pour nous, mais nous mettons maintenant en place une couche intermédiaire qui est une couche logicielle réseau destinée à adresser tous les défis réseau.

Que représente dans ce cadre la souveraineté pour nous ? Chez Nokia, nous voyons arriver toutes les notions de cybersécurité et de sécurité technique à mettre en place. Nous n'avions pas à le faire auparavant puisque nous nous occupions d'avoir des boîtes très sécurisées en entrée et en sortie puis nous les interconnections. Nous aurons maintenant des logiciels sur des plateformes de *cloud*. Ces logiciels sont pour l'instant monofournisseurs mais pourront être multifournisseurs dans le futur. Ils hébergeront des bouts d'applicatifs automobiles, d'applicatifs pour l'énergie… Nous devrons de ce fait assurer de bout en bout une cybersécurité extrêmement élevée pour que ces réseaux virtualisés ne puissent pas s'effondrer. De nouveaux sujets de cybersécurité apparaissent donc, différents des sujets traditionnels.

En tant qu'équipementier de bout en bout, de fournisseur de réseau pour les opérateurs et les grands marchés verticaux comme la SNCF, nous devrons rentrer dans ce domaine de la cybersécurité logicielle pour les logiciels réseau. Cela explique pourquoi il faut porter une attention particulière aux réseaux 5G.

La question de la souveraineté élargit énormément le débat. Il peut s'agir de souveraineté économique pour l'Europe, donc de savoir si nous pouvons nous fournir pour ces infrastructures critiques de façon sécurisée. Ensuite, les États partout dans le monde commencent à se demander si ce qu'ils mettent en place assure la sécurité de leur économie, de leur défense… Nokia n'est pas responsable de ces activités mais responsable du fait de fournir une infrastructure critique sécurisée de bout en bout. Nous nous intéressons à l'aspect technologique et c'est la raison pour laquelle j'ai d'abord décrit ce qu'est un réseau virtualisé. Notre rôle est de fournir à nos clients des infrastructures critiques sécurisées d'un point de vue technologique.

Je n'ai pas bien compris votre question sur la bataille normative. Au niveau de l'infrastructure critique, la 5G est très normalisée. Les différents acteurs mondiaux participent à cette normalisation de l'infrastructure réseau. Nous connaissons déjà les différentes normes à venir pour la 5G : celles de l'année prochaine, de l'année suivante… À ma connaissance, à quelques détails près, nous produisons des équipements tous interconnectables et tous

normalisés selon la même norme. Ce n'est pas comme dans le domaine de la vidéo où coexistent des normes asiatique, européenne et américaine.

M. Philippe Latombe, rapporteur. Lorsque j'ai parlé de bataille normative, je pensais à ce qu'il s'est passé en France avec la loi de 2019 sur la sécurité des équipements qui, notamment pour Huawei, posait des problèmes pour savoir si les mêmes équipements pouvaient être conservés. Je ne parlais pas seulement des normes techniques et technologiques mais aussi des normes d'équipement.

M. Marc Charrière, directeur des affaires publiques de Nokia. En tant qu'équipementier, nous assurons des sécurisations plus que maximales de nos équipements. Je ne donne pas cher de l'avenir d'un équipementier qui sortirait un produit virtualisé non sécurisé.

Les États doivent regarder comment ils bâtissent leur sécurité d'État. Nous n'avons bien évidemment aucune notion de ce qu'il se passe dans les équipements de nos concurrents et ce n'est pas à nous de le faire. Nous ne sommes pas étonnés que des structures de sécurité de l'État analysent nos équipements et que cela concerne les trois équipementiers présents autour de la table. Il ne s'agit pas d'une bataille normative mais d'analyser les solutions mises en place chez nos clients. Nous n'avons ni activité spécifique ni avis à partager sur ce sujet parce que nous ne connaissons pas les équipements des autres.

La 5G n'est pas simplement une évolution de la 4G. Certes, du point de vue du grand public, la première version de la 5G est précisément l'évolution de 4 à 5 et ce que nous allons connaître en 2020 est typiquement une évolution classique avec dix fois plus de débit, dix fois moins de latence. Toutefois, le véritable enjeu est lié aux versions ultérieures.

Pour que nous puissions avoir un véhicule autonome, il faut que le réseau ne fasse pas que des interconnexions. Nous ne pouvons pas développer un applicatif de véhicule autonome et téléphoner à Orange ou SFR en leur demandant un bon réseau, qui aille suffisamment vite pour que la voiture soit autonome. Il faut mettre en place une structure logicielle entre les deux qui sera une sorte de mélange entre des fonctions réseau et des fonctions voiture, d'où l'aspect virtualisation et l'implication de nouveaux acteurs de part et d'autre. En tant qu'équipementiers, nous serons de nouveaux acteurs pour le secteur de l'automobile et le secteur de l'automobile sera un nouvel acteur dans l'aspect réseau. Nous définirons ensuite dans le réseau des « *slices* », c'est-à-dire des couches spécifiques pour un secteur. Le réseau deviendra ainsi intelligent parce qu'il saura ce qu'il transporte. S'il s'agit juste de vidéo, il transportera les données le mieux qu'il peut mais, si c'est une voiture, il faut qu'il sache appuyer sur le frein au bon moment.

Ces aspects sont totalement nouveaux. La bataille économique cache la forêt de l'aspect technologique, très important, qui nécessite beaucoup d'efforts de la part à la fois des équipementiers, des opérateurs et des secteurs industriels eux-mêmes. C'est une rupture à venir, névralgique pour les États car ceux qui ne se plongeront pas dedans rapidement risquent de devenir de simples utilisateurs d'applications développées ailleurs. Nous l'avons déjà vu avec les GAFAM. Il serait bon de ne pas renouveler le problème pour les approches industrielles, en particulier en France où nous avons de gros acteurs qui sont des poids lourds dans le domaine de l'énergie ou d'autres.

M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson. Je souscris à ce qui a été dit sur la partie souveraineté.

Je pense que la souveraineté est un vaste sujet, dont je n'ai pas l'ambition d'avoir la définition absolue et exhaustive. Néanmoins, il me semble que c'est une forme de maîtrise de son destin. Cette maîtrise de son destin passe probablement par une maîtrise de la régulation, une capacité à imposer en partie sa régulation. Je pense que le règlement général sur la protection des données (RGPD) est un exemple de cette volonté d'asseoir sa souveraineté.

Cette souveraineté est aussi associée à une forme de maîtrise technologique. Nous ne pouvons pas bâtir notre souveraineté uniquement sur la réglementation. Par exemple, dans le domaine de l'automobile, nous sentons bien qu'un pays qui n'a aucun constructeur automobile, pas beaucoup de routes, ne peut pas imposer des règles du code de la route ; elles arriveront d'ailleurs. Je veux dire qu'imposer des règles du code de la route numérique ne peut se faire qu'en ayant une forme de maîtrise technologique. Sinon, ce ne sera qu'un rideau de fumée. Pour nous, la maîtrise technologique est un élément constitutif important de la souveraineté comme nous le voyons dans les grands blocs asiatique ou nord-américain.

Il ne faut surtout pas oublier que cette souveraineté, au moins à notre sens, doit être vue comme ouverte et ambitieuse. L'idée n'est pas de construire des murailles, de s'enfermer derrière les murs de son château et de penser que nous avons atteint une solution. Cette souveraineté doit être ouverte, collaborative. L'Europe doit apporter des briques technologiques, une vision mais en restant ouverte aux autres parties du monde.

Ericsson est un acteur européen ; nous faisons 60 % de notre recherche et développement (R&D) en Europe mais nous sommes aussi présents dans 180 pays et, pour nous, il est important d'avoir un accès ouvert à tous ces pays, à tous ces marchés.

S'agissant de la crise covid, notre secteur est plutôt résilient. Le trafic sur les réseaux de télécommunication a augmenté. Les opérateurs français ont à notre sens mieux résisté que d'autres opérateurs. Je suis chargé d'une zone géographique qui comprend la France mais aussi la Belgique, le Luxembourg, l'Algérie, la Tunisie. Je suis d'assez près ces marchés et nous avons vu avec les derniers résultats trimestriels que les opérateurs français ont plutôt bien résisté. Nous en sommes très heureux. C'est important pour nous puisque nous dépendons de leur bonne santé. Les fondamentaux sont bons, le trafic sur les réseaux ayant plutôt augmenté.

Dans d'autres pays, les opérateurs ont moins bien résisté car le confinement ne pousse pas au lancement de nouvelles offres, au renouvellement des forfaits, au renouvellement des terminaux. Certains projets de déploiement d'infrastructures réseau peuvent être gênés. Cela n'a pas été le cas en France où le déploiement a assez bien fonctionné. Par comparaison avec d'autres secteurs, il serait inapproprié que je m'étende plus longuement sur nos malheurs alors que nous résistons globalement bien.

La sécurité est un sujet croissant car nous sommes encore plus dépendants des réseaux en 5G qu'en 4G. En 4G, si je perds la connexion, que l'image se fige ou qu'une panne fait tomber le réseau, c'est évidemment moins grave qu'avec la 5G, avec des automobiles connectées et des industries qui s'appuient dessus.

Nous pouvons d'abord voir la sécurité sous l'angle des standards définis collectivement au sein du *3rd generation partnership project* (3GPP) pour concevoir les solutions les mieux sécurisées. Dans ce sens, la 5G est montée sur les épaules de ses prédécesseurs 4G et 3G pour créer des solutions encore plus avancées.

Le deuxième angle de la sécurité est le fait que chaque équipementier décide de concevoir ses produits et d'intégrer ses standards de sécurité dans ses produits, en complétant avec ses méthodes. Chacun essaie de faire au mieux sans trop savoir ce que font les autres.

C'est aux autorités telles que l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dans les différents pays, de regarder ce que chacun a créé.

Le troisième point est la façon de déployer les réseaux, avec des *firewalls* (pare-feu), de bons réseaux privés virtuels (VPN), de bonnes fonctionnalités de cryptage. La responsabilité est partagée entre l'équipementier et l'opérateur.

Le quatrième point est la manière d'opérer ces réseaux. Si, en ayant pris les précautions précédentes, j'écris le mot de passe sur le tableau derrière mon bureau, ce bel édifice sera un peu gâché. Tout cet ensemble est constitutif de la sécurité, aussi bien au sens de la protection contre des pirates que de la résilience face à des pannes.

Un autre volet qui revient souvent dans les discussions concerne la confiance. Il faut que j'aie confiance dans les différents acteurs de la chaîne. C'est la métaphore du serrurier : il m'a fait la meilleure serrure du monde pour ma maison mais il a gardé un double des clés et je n'ai pas confiance en lui.

Le dernier pilier est la souveraineté : pour être pleinement souverain, comprendre ce qu'il se passe, il faut aussi que j'aie une forme de maîtrise sur certaines des briques de la solution numérique globale.

La 5G est un moteur des activités d'Ericsson. Nous fournissons actuellement 70 réseaux commerciaux 5G dans le monde. L'association globale des équipementiers (GSA) dont font aussi partie mes homologues a recensé 125 réseaux ouverts commercialement en 5G dans le monde dans 52 pays. L'évolution est donc rapide et je pense que déployer ces réseaux est un enjeu de compétitivité pour la France et pour l'Europe. Être capable de déployer la 5G et de l'utiliser est aussi un enjeu pour l'industrie. Cela passe également par des usages grand public.

Un énorme enjeu pour nous, qui nous a beaucoup occupés cette année, est de communiquer sur la partie environnementale. Des craintes ont été soulevées. Il est légitime de s'inquiéter de l'impact environnemental de ce que nous faisons. Nous pensons qu'il existe aussi beaucoup de *fake news*, de distorsions de la réalité. Nous essayons de faire de la pédagogie pour montrer que la réalité est différente, que l'impact est plutôt stable et que nous pensons qu'il existe des moyens de déployer des réseaux 5G sans accroître l'impact carbone des réseaux. De plus, la 5G apporte des leviers tout à fait intéressants pour réduire l'impact carbone d'autres secteurs.

Mme Linda Han, déléguée générale de Huawei France. D'après le rapport du Sénat de 2019, la souveraineté numérique comprend trois aspects : la souveraineté technologique, la souveraineté industrielle et la souveraineté de la donnée. En nous basant sur cette compréhension de la souveraineté, la volonté de bâtir une autonomie stratégique et de relocaliser l'industrie, nous portons notre réflexion plutôt sur la façon de bien nous adapter à cette souveraineté numérique.

Notre première réponse est donc de tenir compte de ce souhait de relocalisation. Nous avons déjà cinq centres de recherche et développement (R&D) en France ainsi qu'un centre de recherche fondamentale qui dépose chaque année 50 brevets en France. De plus, nous nous approvisionnons en « Made in France » et, rien qu'en 2019, nous avons acheté pour plus d'un milliard de dollars américains de produits et de services en France. En ce qui concerne le « Made in Europe », nous avons décidé de créer une usine en Europe et cette usine doit s'installer en France. Tous les produits 2G, 3G, 4G, et 5G seront donc fabriqués en France.

Notre deuxième réponse porte sur la souveraineté des données. Nous avons bien compris que toutes les données doivent rester en Europe et en France. Toutes les données soumises au RGPD restent en France. Nous nous préoccupons aussi de la sécurité des équipements en concevant et en fabriquant nos produits selon un processus interne qui garantit la sécurité.

Nous avons également compris qu'il faut établir la confiance entre Huawei et toutes les tierces parties partout dans le monde. En France, nous testons tous nos équipements 5G avec Thalès en présence de l'ANSSI, en utilisant les standards de l'ANSSI, pour montrer que nos produits ne posent aucun problème de sécurité. Nous avons plus de 223 certificats délivrés par des tiers après vérification des équipements de Huawei. Ces certificats ont été délivrés en particulier par Thalès et, en Allemagne, par l'Office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik*, BSI).

Je partage entièrement le point de vue d'Ericsson selon lequel la souveraineté doit aussi être ouverte et collaborative. Il faut construire un environnement dans lequel tous les acteurs puissent contribuer à la construction de cette future souveraineté et de l'économie.

Nous sommes comme tout le monde impactés par la covid-19. Nous avons pris beaucoup de précautions pour assurer la santé de tous nos employés et pour faire en sorte que les stocks, les équipements puissent être acheminés à temps vers tous les pays. La covid-19 a aussi un gros impact sur la digitalisation. Elle accélère le rythme de la digitalisation et de l'innovation.

Durant le premier confinement, en France, nous avons constaté une augmentation de 30 % du trafic chez les opérateurs. Nous avons mobilisé plus de 200 ingénieurs français pour qu'ils aillent dans les régions, qu'ils accompagnent les opérateurs pour garantir la qualité du réseau et pour fournir une très bonne connexion durant cette période. Nous avons aussi lancé le programme Digital InPulse pour encourager l'innovation dans les territoires français.

Ericsson et Nokia ont déjà largement abordé la question de la 5G. Nous pensons qu'il est toujours mieux de travailler ensemble pour résoudre certaines suspicions ou certains problèmes techniques. Il faut travailler ensemble pour construire un standard beaucoup plus clair et plus transparent, ainsi qu'un règlement commun à toute l'industrie afin de bien réguler toutes les contraintes de sécurité.

Nous ne comprenons pas de nombreux points dans les décisions prises car nous n'avons pas accès à la décision. Nous ne savons pas si la décision est un refus de Huawei ou s'il est moins facile de donner des autorisations à Huawei. Nous essayons de voir comment établir un environnement meilleur pour tous afin de mieux déployer cette technologie.

Nous avons 1 000 employés en France et nous sommes présents pour assurer que nous pouvons faire rapidement le déploiement de la 5G. Les investissements que nous avons faits en R&D permettent que cette technologie consomme moins d'énergie. Nous sommes là pour accompagner nos clients afin de déployer le réseau au plus vite et avec la meilleure qualité possible. Nous sommes prêts à faire preuve de toute la transparence nécessaire, à faire plus de tests en commun.

M. Minggang Zhang, directeur général adjoint de Huawei France. De notre point de vue, la 5G est d'abord une infrastructure et une technologique pour construire un réseau. La 5G est une rupture par rapport aux précédentes générations, notamment dans la capacité de connexion, la vitesse et la latence, ce qui la rend extrêmement puissante pour développer différentes solutions.

Nous avons parlé des réseaux virtualisés, des *slices* et tout cela est construit sur une infrastructure réseau très normalisée au-dessus de laquelle nous avons différentes possibilités pour déployer des applications telles que des véhicules autonomes, des villes intelligentes… Nous aurons alors besoin, par secteur, de travailler de bout en bout sur des réseaux d'applicatifs. Nous avons donc un réseau au sens de l'infrastructure avec différentes possibilités d'applications.

Huawei ne prétend pas être un acteur couvrant l'intégralité des applications 5G. Notre stratégie est de rester le fournisseur de solutions technologiques aussi performantes que possible et de travailler sur des solutions applicatives dans les différents secteurs avec nos partenaires dans le monde entier.

La question de la cybersécurité est pour nous avant tout une question technique. Nous avons constaté durant la période de la covid une augmentation extrêmement rapide de la demande sur les réseaux. Si les opérateurs français résistent relativement bien, mieux que certains autres, je pense que cela montre que leur base en matière de sécurité est solide. Les opérateurs français sont capables de bien gérer le réseau.

La loi traduit une réglementation que l'État français souhaite mettre en place et nous souscrivons à cette démarche. En tant que fournisseur de technologie, il est important que nous respections les différents standards. La souveraineté comprend aussi une partie liée au cahier des charges ; l'ancienne secrétaire générale de la défense nationale, Mme Claire Landais, avait précisé que l'État doit rester maître des décisions et des valeurs dans une société numérisée. Enfin, la souveraineté contient une partie de volonté politique qui est liée à la réglementation.

Tout ceci doit s'inscrire dans un contexte d'ouverture et de collaboration. Actuellement, plus personne ne maîtrise de A à Z toutes les technologies, ce qui rend nécessaire l'ouverture et l'esprit de collaboration. L'ensemble doit être assis sur une base de sécurité et de cybersécurité bien construite.

Mme Laure de La Raudière. Pour moi, la souveraineté tient aussi à notre capacité à nous approvisionner pour fabriquer sur le territoire européen nos propres équipements. J'ai bien entendu la remarque de Huawei qui dit que nous avons une souveraineté parce que nous avons constitué des stocks.

La constitution de stocks est-elle aussi pratiquée chez Nokia et Ericsson ? Quelle est votre part d'autonomie par rapport à vos sous-traitants en matière de *sourcing* ? Avoir des partenaires européens est bien mais si l'ensemble des équipements ou des parties de vos équipements sont achetés hors d'Europe, nous pouvons être contraints dans certains cas à ne plus être souverains. Nous l'avons déjà vu dans d'autres filières économiques, en particulier sur les médicaments durant la crise sanitaire, mais le même phénomène pourrait se produire dans le domaine des télécoms dans un futur où nous ne maîtriserions pas nos chaînes de production.

M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson. Nous sommes également dans cette logique de production par zone géographique. Nous avons des usines en Asie, en Amérique et nous produisons aussi en Europe, plutôt en Estonie et en Pologne, mais avec l'idée de produire une grande partie de nos équipements pour le marché européen en Europe. Nous procédons de même pour les autres plaques géographiques. Il s'agit de réduire les temps d'approvisionnement, d'être plus flexible.

Ces usines sont des usines d'assemblage et, effectivement, utilisent beaucoup de composants. Nous avons appris des crises passées car il s'est produit ces dernières années des tensions sur le marché des composants actifs. Il est arrivé que nous ne puissions pas servir complètement tous les clients en temps et en heure. C'est lié au fait que d'autres industries comme l'industrie automobile se sont également beaucoup digitalisées et ont demandé beaucoup de composants.

Cette question de l'approvisionnement en composants actifs n'est donc pas nouvelle. De ce fait, nous constituons des stocks pour nous affranchir des risques associés à une sur-demande ponctuelle du marché. Par ailleurs, nous avons choisi de diversifier nos sources. Nous n'avons pas un seul fournisseur qui peut, soit avoir un problème, soit avoir une demande très forte et être obligé de faire des arbitrages pour fournir ses clients. Nous avons donc une production locale, des stocks et du *sourcing* élargi.

M. Marc Charrière, directeur des affaires publiques de Nokia. Nous avons un peu près les mêmes stratégies d'approvisionnement. J'ajoute qu'il ne faut pas confondre les terminaux et les équipements de réseaux. Nokia n'est pas fournisseur de terminaux.

Mme Laure de La Raudière. Je parlais vraiment des équipements de réseau, pas des terminaux.

M. Marc Charrière, directeur des affaires publiques de Nokia. Il est important de distinguer les deux car la situation est très différente. Sur les réseaux, nous sommes vraiment des fournisseurs de logiciels et l'équipement est de plus en plus de l'équipement logiciel. Le *hardware* devient de plus en plus banalisé. Avec une approche multifournisseur et multisource pour l'intégration, la valeur ajoutée est vraiment dans le logiciel et Nokia passe un pourcentage énorme de son chiffre d'affaires en développement logiciel. Il faut donc savoir où sont développés les logiciels, s'ils sont développés sur plusieurs sites dans le monde, si nous sommes capables de nous retourner au niveau du développement logiciel, si nous sommes présents dans plusieurs pays.

Pour la fourniture du *hardware*, des *Application-Specific Integrated circuit Chips* (ASIC), Nokia a de multiples sources, voire des sources en propre pour certains ASIC que nous développons nous-mêmes, et nous avons également du stock. Notre gestion est d'abord européenne, mondiale ensuite. Nous ne développons pas tout à partir d'un ou deux pays ni d'un ou deux continents. L'approche est mondiale, multi-source et multi-continent.

Il faut ensuite implanter le logiciel mais la valeur ajoutée sur les équipements réseau est souvent inférieure à la valeur ajoutée sur les équipements terminaux. Dans les terminaux, l'électronique est entièrement intégrée car il faut que tout tienne dans une petite boîte. Sur les réseaux, la fourniture des ASIC est importante mais nous avons toujours des solutions de contournement.

Mme Linda Han, déléguée générale de Huawei France. Nous avons 300 fournisseurs en France et nous y avons fait pour un milliard de dollars d'achats en 2019. Nous avons 3 100 fournisseurs en Europe et nous y avons acheté pour plus de 8,3 milliards de dollars en 2019.

S'agissant de la production, notre usine en Europe est destinée non seulement à l'assemblage des composants que nous achetons mais aussi à la fabrication de parties de la carte-mère pour la technologie 5G.

Sur la partie logicielle, Huawei accorde une très grande importance à la R&D. En 2019, nous avons investi plus de 18,2 milliards de dollars en R&D. En plus des centres de R&D dont j'ai déjà parlé en France, nous avons en Europe 23 centres de R&D situés dans quatre pays européens.

Nous avons commencé à investir sur la technologie 5G dès 2009 et nous avons déjà investi au total plus de 4 milliards de dollars sur cette technologie. Cela nous permet d'avoir une certaine avance technologique.

M. Minggang Zhang, directeur général adjoint de Huawei France. Du côté de Huawei, nous restons relativement centrés sur l'infrastructure et les terminaux. Nous développons beaucoup nos propres technologies, en respectant bien évidemment les normes et les standards internationaux.

De notre point de vue, dans les solutions les plus pointues aujourd'hui en matière de télécommunication, le *hardware* continue à jouer un rôle important voire très important. Ceci ne signifie pas que nous ne développons pas de logiciel ; nous développons bien des logiciels de télécommunication qui gèrent et font fonctionner les équipements.

Sur la partie approvisionnement, nous avons une politique multi-source, sur les différents continents, en Europe, au Japon, en Chine, en Corée… Cette politique multi-source et notre politique de R&D nous permettent d'assurer un approvisionnement mieux réparti dans différentes parties du monde.

Mme Laure de La Raudière. Il serait intéressant que nous ayons un écrit sur les détails de ce *sourcing* et de cette production sur le territoire européen pour les parties logicielle et *hardware*. C'est pour moi un élément de souveraineté. Nous sommes fiers d'avoir des entreprises européennes dans ces secteurs mais la souveraineté peut aussi être que nous maîtrisions bien la production de ces éléments essentiels que sont les éléments réseau.

M. Philippe Latombe, rapporteur. Nous avons auditionné les opérateurs de télécommunications dont certains nous expliquaient avoir des soucis pour implanter la 5G en France car certains élus locaux n'y étaient pas favorables, avaient demandé des moratoires… Comment voyez-vous ce mouvement de défiance vis-à-vis de la 5G ? Est-ce justifié ou non ? Constatez-vous ce même sentiment de défiance dans d'autres pays européens ou est-ce franco-français ?

La souveraineté n'est peut-être pas qu'une question de technologie et de réglementation mais aussi d'acceptation par la société d'évolutions techniques et de mesures de protection. La société française semble aujourd'hui un peu divisée sur la 5G.

M. Viktor Arvidsson, directeur des activités relations institutionnelles, innovation et stratégie d'Ericsson. Je souscris à ce qui a été dit par mes concurrents sur l'importance de la partie logicielle.

Sur la partie environnementale, il semble que ce soit un phénomène français, peut-être francophone puisque nous le voyons aussi en Belgique où c'est un sujet assez fort, beaucoup repris dans la presse. Je comprends les problèmes de nos clients opérateurs et je pense qu'il faut que nous travaillions dessus. Il me semble que c'est une combinaison de mauvaises perceptions de la réalité et qu'il faut poursuivre le dialogue déjà entamé.

L'impact carbone actuel du numérique est mal perçu, l'impact du *streaming* est également mal perçu. Les gens ne connaissent pas suffisamment le gain qu'apportera la 5G, qui est de l'ordre d'un facteur 10 pour la même quantité de données. Je pense qu'un effort de communication est à faire mais que nous sommes peut-être aussi dans un contexte un peu

technophobe que nous avons du mal à appréhender parce que nous sommes naturellement technophiles.

Une question de fond est malgré tout légitime : celle de l'effet rebond. Les gens veulent bien nous croire sur le fait que la 5G est dix fois plus efficace mais pensent que, du fait de cette efficacité supplémentaire, malgré les gains de productivité, un effet rebond se produira avec une boucle de surconsommation et que le résultat final sera plus mauvais qu'au départ. Je pense que c'est là le débat réellement intéressant.

Il existe des effets rebond négatifs dans tous les domaines. Par exemple, si j'augmente la performance de l'agriculture, je produis plus de viande, j'augmente la quantité de protéines animales et j'ai un impact négatif. Ce phénomène n'est pas intrinsèque au numérique. Je trouve délirant le constat que j'entends selon lequel, puisqu'il peut exister un effet rebond, il ne faut plus bouger, ne plus rien faire et rester dans la technologie actuelle, alors que le monde autour de nous bouge et que nous risquons de prendre du retard dans la compétition.

Gagner en productivité est vieux comme le monde. Quand l'homme a domestiqué le feu voici 400 000 ans, il a bénéficié d'un gain de productivité dans sa mastication. Quand il a inventé la roue, il a eu un gain de productivité et ce phénomène se répète tous les ans depuis des dizaines de milliers d'années. S'arrêter maintenant n'est en rien une solution par rapport à l'histoire de l'homme, au génie de l'humain et n'est pas une solution dans un contexte concurrentiel.

L'université de Zurich a sorti un rapport assez intéressant sur la 5G. Ce rapport propose de voir quels sont les effets positifs de la 5G pour d'autres secteurs, d'identifier de manière itérative les effets rebond et de voir comment ces effets rebond peuvent être traités. Ils peuvent être traités par la réglementation, par une incitation à d'autres formes d'usage. Par contre, décider de ne rien faire à cause de l'effet rebond est délirant.

Pour donner un exemple concret, ce rapport indique que la 5G peut apporter beaucoup de progrès pour l'automobile connectée. Un effet rebond potentiel de l'automobile connectée et autonome est que, après pris ma voiture pour aller travailler au bureau, je la renvoie chez moi parce que je ne trouve pas de place pour me garer à côté du bureau puis je lui ordonne de revenir me chercher, ce qui pourrait doubler le nombre de trajets en automobile. Ce serait un effet rebond négatif qu'il faut éviter mais ce n'est pas pour cette raison qu'il faut éviter de créer des automobiles connectées qui pourraient avoir de nombreux effets positifs induits. Il faut prévoir une forme de réglementation, par exemple une incitation à un partage des véhicules pour éviter l'effet rebond négatif.

C'est un vrai sujet, un peu spécifique à la France. D'autres pays très conscients de l'environnement comme en Scandinavie n'ont pas ce problème. Les deux axes de travail sont de communiquer sur la réalité de la 5G et d'attaquer le nœud du problème, en particulier ces effets rebond qu'il faut travailler en faisant en sorte de les éviter mais qui ne doivent pas être un frein.

M. Marc Charrière, directeur des affaires publiques de Nokia. Je souscris complètement à ce qui vient d'être dit. Sur l'aspect sociétal, c'est effectivement un sujet très français. Je pense que nous sommes un peuple très innovant mais qui a besoin d'avoir fait le tour en théorie de ce qu'il se passera, avec des chiffres, de gains… Or, la 5G apportera une évolution très forte surtout dans les secteurs industriels, donc des gains.

Par exemple, les champs éoliens gérés un par un nécessitent actuellement un lissage de l'énergie avec souvent des centrales thermiques. Le déploiement d'une infrastructure numérique évoluée avec la 5G et d'autres technologies permettra de mieux gérer les parcs

éoliens. Il faut commencer à expérimenter pour voir ce que cela donnera. Dans d'autres pays, en particulier dans le nord de l'Europe, la réaction est de tester en ayant en tête le fait qu'il faut faire attention à l'environnement. Si la 5G conduit à un échec sur les champs éoliens, ils reviendront en arrière. En France, nous voulons avoir fait toute l'analyse complète avant de mettre les bottes et d'aller sur le terrain. Nous avons donc beaucoup de mal à voir les effets positifs, à faire des tableaux Excel avec les effets positifs, négatifs et à voir que, finalement, l'impact est positif dans l'exemple que je viens de citer.

Il faut que nous expérimentions plus et plus longtemps, pas uniquement pour montrer que notre site d'expérimentation 5G fait dix fois plus de ci, dix fois moins de ça… L'expérimentation avec les secteurs industriels est extrêmement importante et des pays le font. C'est important pour notre développement économique et pour notre développement durable à venir.

Notre approche doit être plus pratique, pragmatique plutôt que d'appuyer sur le frein. En France, nous appuyons sur le frein pendant des années puis nous le lâchons et, d'un seul coup, nous fonçons sur la technologie. Toutefois, nous risquons de prendre ainsi du retard dans la mise en œuvre tandis que, dans la mise à disposition des fréquences, nous ne sommes pas à six mois près puisque le développement durera des années.

Nous voulons trop tout analyser à l'avance, avec des partis pris trop négatifs. Il faut avancer et je ne doute pas que cela avancera. Les autres pays d'Europe ne nous comprennent pas bien d'ailleurs.

Mme Linda Han, déléguée générale de Huawei France. Pour la même quantité de données, la technologie 5G consomme dix fois moins d'énergie que la 4G. La consommation de chaque site est à peu près inchangée mais la capacité de la 5G est beaucoup plus grande.

Dans les travaux de R&D, Huawei s'est déjà beaucoup préoccupé de la protection de l'environnement. Ainsi, les sites de 4G sont très grands et nous avons essayé de consommer moins tout en faisant plus pour la 5G. Nous arrivons ainsi à construire des équipements 5G beaucoup plus petits. Nous avons par exemple un organe 5G qui ne pèse que vingt kilogrammes et peut être installé très facilement. Nos sites 5G consomment aussi moins d'énergie qu'en 4G.

Nous avons déjà l'expérience de 91 contrats de 5G et nous savons accompagner nos clients pour réaliser des installations très rapides. En tant que fournisseur d'équipement, nous pouvons faire des efforts pour assurer que les déploiements des opérateurs soient aussi rapides que possible.

M. Jean-Christophe Aubry, responsable des affaires publiques de Huawei. Je pense qu'il faut distinguer souveraineté et acceptabilité. La souveraineté est la défense des intérêts nationaux tandis que l'acceptabilité est liée à une perception du citoyen, à l'expression d'une réticence et de craintes face à un changement important.

La technophobie générale à laquelle nous faisons face n'est pas nouvelle en France. Nous l'avons vue sur la 4G, sur Linky, sur l'implantation d'éoliennes. Ce principe a été théorisé par l'acronyme Nimby, *Not in my backyard*. Il faut impérativement traiter ces deux questions mais elles sont à distinguer. L'acceptabilité sociale n'est pas une question de souveraineté ; il s'agit de rassurer le citoyen face à un changement.

M. Philippe Latombe, rapporteur. Je vous remercie et j'attends vos contributions sur la partie sous-traitance et *sourcing*.

Audition, ouverte à la presse, de M. Jacques de Heere, vice-président du comité stratégique de filière (CSF) « Infrastructures numériques » et président du groupe industriel ACOME, M. Michel Combot, délégué permanent du CSF, M. Aubin Bernard, chargé de mission à la Fédération InfraNum, Mme Marie-Thérèse Blanot, représentant le Syndicat professionnel des fabricants de fils et de câbles électriques et de communication (SYCABEL), et M. Jugwal Doyen, représentant la Fédération française des télécoms
(3 décembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. Philippe Latombe, rapporteur. Nous recevons les membres du Comité stratégique de filière (CSF) « Infrastructures numériques » : M. Jacques de Heere, vice-président du comité stratégique de filière (CSF) « Infrastructures numériques » et président du groupe industriel ACOME, M. Michel Combot, délégué permanent du CSF, M. Aubin Bernard, chargé de mission à la Fédération InfraNum, Mme Marie-Thérèse Blanot, représentant le Syndicat professionnel des fabricants de fils et de câbles électriques et de communication, le SYCABEL, et M. Jugwal Doyen, représentant la Fédération française des télécoms

Cette audition s'inscrit dans le cadre des réflexions que nous souhaitons mener sur la souveraineté de nos infrastructures numériques. Nous avons en effet déjà auditionné les opérateurs et équipementiers. Nous profitons de votre présence aujourd'hui pour continuer à aborder la partie « *hardware* », c'est-à-dire la production et l'installation des composants physiques de nos infrastructures numériques.

Je voudrais d'abord vous interroger sur le sens que revêt pour vous la notion de souveraineté numérique au sein de votre secteur d'activité. Ce concept, parfois rapproché de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique, de ne pas subir les contraintes imposées par certains acteurs publics comme les États ou privés comme les géants du Web, les GAFAM. Je souhaite savoir quel regard les acteurs de l'industrie du numérique et des infrastructures portent sur cette préoccupation croissante des pouvoirs publics.

Je voudrais également vous entendre sur les enjeux technologiques du numérique. La crise de la covid a montré combien la résilience de nos infrastructures numériques est essentielle pour la continuité de l'activité économique et des services publics. J'aimerais que nous évoquions ensemble non seulement l'impact de la crise de la covid sur vos activités mais aussi votre perception des secteurs technologiques sur lesquels notre pays doit conserver une autonomie stratégique pour éviter d'être pris en défaut en cas de crise. Cette interrogation rejoint l'idée d'une forme de souveraineté technologique française ou européenne qui a été au cœur des réflexions menées dans le cadre du plan de relance et du plan d'investissements d'avenir.

Nous travaillons aussi au sein de cette mission d'information sur les aspects économiques de la souveraineté numérique. Ils concernent aussi bien la fiscalité que l'émergence d'acteurs français ou européens capables de lutter à armes égales avec nos concurrents extra-européens. Nous serions donc intéressés par votre vision de l'action menée par les pouvoirs publics pour soutenir votre secteur d'activité et d'éventuelles pistes ou recommandations de nature à améliorer encore les dispositifs existants.

M. Jacques de Heere, vice-président du comité stratégique de filière (CSF) « Infrastructures numériques ». Le comité stratégique de filière « Infrastructures numériques » a été labellisé en 2018 par le Conseil national de l'industrie. Il est constitué de très nombreuses entreprises, des fabricants de câbles, des industriels des équipements, des installateurs, des constructeurs de réseaux et d'infrastructures et des opérateurs télécoms. Il rassemble quatre grandes fédérations professionnelles. Son ambition est de connecter les citoyens et de contribuer au développement des usages innovants dans les territoires au bénéfice de tous et de toutes.

Cette vocation se traduit dans les chiffres et les moyens. Chaque année, des milliards d'euros sont investis dans la construction des réseaux de demain. La plus grande partie de ces investissements provient actuellement des opérateurs de télécommunications eux-mêmes. Les investissements en recherche et développement sont également très importants pour répondre à l'évolution des technologies, notamment la 5G mais aussi à l'avènement des « territoires intelligents », les *smart* territoires.

Le CSF « Infrastructures numériques » s'est organisé autour d'instances qui travaillent en permanence sur les enjeux de demain : les fédérations professionnelles, les entreprises du secteur, les syndicats de salariés, l'État, les collectivités, des associations représentatives. Le contrat de filière qui a été signé a retenu quatre projets ambitieux : rendre accessible à tous et toutes les réseaux de 5G en passant par la mise en œuvre d'un réseau de plateformes ; construire des territoires intelligents ; favoriser l'emploi et le développement des compétences ; et rendre cette filière visible à l'international pour construire une stratégie d'offre à l'exportation.

Un réseau de plateformes s'est mis en place pour développer la 5G. Des opérations à travers les territoires pour sensibiliser et mobiliser les collectivités territoriales ont commencé.

Mme Marie-Thérèse Blanot, déléguée générale du Syndicat professionnel des fabricants de fils et de câbles électriques et de communication (SYCABEL). Le SYCABEL représente des entreprises qui interviennent dans deux types des métiers. Le premier est celui de l'électricité puisque nous fabriquons tous les câbles et matériels de raccordement pour les réseaux électriques, le transport et la distribution d'électricité. Nous amenons donc l'électricité dans les bâtiments en essayant de développer des matériaux qui protègent les biens et les personnes vis-à-vis du feu, en particulier dans les centrales nucléaires et les chantiers navals. Le deuxième concerne tous les câbles et accessoires télécoms. Nous avons bien sûr été à l'origine du réseau cuivre puisque nous avons fabriqué tous les câbles et nous sommes maintenant concernés par les câbles à fibres optiques pour le déploiement du réseau France Très Haut Débit.

Les câbles sont mal connus ; ils sont souvent cachés, enterrés ou masqués dans des gaines et des tubes. Ce sont des produits très techniques, très technologiques. Les entreprises de ce secteur sont des entreprises industrielles de process réparties sur le territoire national. Nous en comptons près de quarante. Derrière ces entreprises se trouvent les entreprises de production de fibres optiques et de câbles à fibres optiques qui sont des champions européens parmi lesquels de grands noms comme Nexans ou Prysmian ainsi que de magnifiques entreprises de taille intermédiaire (ETI) dont ACOME. Parmi les adhérents du SYCABEL se trouvent aussi de petites et moyennes entreprises (PME).

M. Michel Combot, délégué général du CSF. J'assure la présentation de l'Alliance française des industries du numérique (AFNUM) puisque sa déléguée générale, Stella Morabito, n'est pas disponible.

L'AFNUM représente l'ensemble du secteur des équipementiers de toute la filière des infrastructures numériques. Ce syndicat a énormément évolué avec la restructuration industrielle de notre secteur. Il existait voici quelques années un grand champion, Alcatel. La situation est aujourd'hui bien différente, même si la vision est beaucoup plus européenne en matière d'infrastructures et surtout d'équipements. Nokia et Ericsson sont parmi les champions mondiaux. Il reste malgré tout des enjeux d'emplois qui ne sont pas évidents compte tenu notamment de la crise que traverse actuellement le groupe Nokia.

L'AFNUM regroupe aussi des petites entreprises et des entreprises du secteur des composants électroniques essentiels pour les infrastructures numériques. Pour la 5G, nous travaillons par exemple avec Sequans, qui d'ailleurs préside l'AFNUM et qui est très présent dans le domaine des objets connectés. Ces fabricants sont pour nous importants notamment en matière de compétitivité et permettent de développer tout un écosystème autour de ces infrastructures.

Outre mes fonctions de délégué permanent du CSF, je suis directeur général de la Fédération française des télécoms. Vous avez déjà auditionné la Fédération qui regroupe les grands donneurs d'ordres que sont les opérateurs. Ces acteurs ne sont pas tout à fait en haut de la chaîne de valeur parce que les acteurs de l'internet se situent tout en haut.

La fiscalité est un enjeu important : toutes ces infrastructures développées par les opérateurs, les installateurs, les équipementiers, les fabricants de câbles profitent aussi à des acteurs qui ne sont pas forcément basés en France et qui bénéficient d'un cadre complètement différent du nôtre. Vous avez autour de la table des acteurs qui paient des impôts en France, emploient des personnes en France. Dans cet enjeu d'équité fiscale, pour redonner de la valeur à l'industrie, avancer en tant que filière est un élément important. Nous avons vu la solidarité interne à la filière lors de la crise et il est important que nous raisonnions en termes de filière. Des emplois et du développement sont en jeu, ce qui est essentiel pour notre pays.

M. Aubin Bernard, chargé de mission à InfraNum. InfraNum est l'une des quatre fédérations qui composent le CSF. Elle a été créée en 2012 pour accompagner le début du plan France Très Haut Débit. InfraNum regroupe aujourd'hui plus de 200 entreprises qui représentent toute la chaîne de valeur du plan France Très Haut Débit, du bureau d'études aux intégrateurs et installateurs en passant par les opérateurs d'infrastructures et les opérateurs de services qui fournissent des services très haut débit et des services aux entreprises françaises.

Nous nous inscrivons parfaitement dans la feuille de route de ce CSF avec nos grands thèmes d'action, dont le déploiement du haut débit partout en France. Nous accompagnons les territoires dans la mise en œuvre de cette infrastructure neutre, ouverte et mutualisée ce qui est en quelque sorte notre devise.

Nous sommes également positionnés sur tous les sujets tels que les territoires intelligents, la gouvernance de la donnée, l'emploi. L'emploi est un sujet particulièrement important pour InfraNum et ses adhérents. Nous réfléchissons aux métiers de l'après-fibre.

Nous sommes aussi très impliqués à l'international, dans la valorisation et la promotion de nos savoir-faire et du modèle des réseaux à la française. Nous portons plusieurs livrables et projets au sein du groupe de travail « International » du CSF.

Enfin, la concurrence fait aussi partie des sujets que porte quotidiennement la fédération InfraNum depuis 2012.

M. Jacques de Heere, vice-président du comité stratégique de filière (CSF) « Infrastructures numériques ». La question de la souveraineté répond évidemment à un enjeu national de grande importance. Au CSF, nous mesurons cette souveraineté à l'aune de la qualité des réseaux construits, de leur pérennité, de leur sécurité. Nous allons vous présenter les réseaux de plateformes et toutes les opérations que nous entreprenons dans les quatre groupes du CSF.

M. Michel Combot, délégué général du CSF. Les sujets de souveraineté ne sont pas totalement évidents et sont liés aux sujets de sécurité. Le secteur des infrastructures numériques s'est énormément développé en France par la concurrence depuis près de vingt-cinq ans, avec l'ouverture à la concurrence guidée par les directives européennes. Nous considérions alors que la concurrence entre plusieurs acteurs permettrait de stimuler l'innovation et d'accélérer le développement, ce qui est bien le cas à l'heure actuelle.

En se plaçant selon le prisme de l'accès aux services de communication électronique, les prix en France sont parmi les plus bas avec des réseaux qui sont parmi les plus performants au monde. C'est un point important car ce n'est pas totalement évident pour une chaîne de valeur qui est en concurrence sur tout le segment.

Pour les câbles, il existe plusieurs constructeurs de niveau européen en concurrence, sans même parler des constructeurs hors Europe. C'est vrai également pour les équipements et encore plus au niveau des opérateurs avec quatre opérateurs en France. Cette concurrence entraîne comme bénéfice la stimulation des investissements et du déploiement. En revanche, elle a pour conséquence que le ratio coût-efficacité est souvent regardé par tous les donneurs d'ordres pour avancer.

Je pense que nous pouvons tous ici converger vers l'objectif suivant : la France doit disposer des infrastructures et surtout d'une industrie la plus performante possible et la moins dépendante des technologies étrangères. Toutefois, nous avons fait face depuis plus de vingt ans à une désindustrialisation très importante sur certains segments de marché, notamment pour les équipementiers. Nous avons certes aussi de bons exemples car le développement des infrastructures a permis de générer le développement d'industriels sur d'autres segments.

Le parti pris au sein de la filière est de transcender ces aspects de concurrence pour essayer de retrouver de l'investissement et du développement sur les points essentiels de nos infrastructures. Notre comité de filière est un peu une exception car d'autres comités sont vraiment gérés par des industriels. Nous avons décidé au sein de notre filière de faire gérer notre CSF par les fédérations parce que nous avions cette habitude de rassembler des acteurs qui peuvent avoir des enjeux concurrentiels très forts. Cela nous permet de trouver une vision commune consistant à investir dans les infrastructures de demain et dans les métiers de demain.

Par exemple, la 5G commence à se développer de manière très concurrentielle entre opérateurs mais nous pensons que certains enjeux dépassent la vision concurrentielle, notamment l'apport de la 5G pour les autres industries. Nous avons donc décidé d'aller ensemble convaincre et démontrer quel peut être l'apport de la 5G pour la modernisation des autres industries dans une optique de relance de notre économie. Nous essayons de trouver ces éléments communs qui permettent d'avancer en créant de l'emploi, en créant du service, en développant des PME et en réindustrialisant notre pays, en tout cas notre vivier de PME et d'industriels. Il s'agit aussi de continuer à créer des débouchés pour nos industriels. Développer ainsi ces emplois, ces infrastructures constitue pour nous la véritable souveraineté, au-delà de l'aspect concurrentiel.

Nokia connaît des difficultés et supprime des emplois. Nous pouvons nous demander comment recréer de la valeur dans ces infrastructures pour permettre de recréer de l'emploi en France. Cela peut être avec de nouvelles infrastructures, de nouveaux métiers, en créant de nouveaux emplois dans l'industrie pour le développement de la 5G dans les industries elles-mêmes. Cela peut être aussi avec les territoires connectés ; il s'agit de prendre en main tous les usages numériques pour créer des services performants dans tous les domaines, aussi bien pour la gestion des services publics de l'eau, de l'énergie que pour la gestion de la donnée publique. L'enjeu est de créer de l'emploi, de créer du service et de moderniser l'ensemble de ces secteurs. C'est encore une question de souveraineté : au lieu d'aller acheter à l'étranger, s'il existe demain une solution française et européenne, ce seront autant d'emplois conservés et notre souveraineté en sera renforcée.

Les débats n'ont jamais été évidents au sein de notre comité de filière car nous sommes par nature très concurrentiels. Les gens font parfois des calculs à très court terme en achetant hors Europe parce qu'ils ont besoin d'augmenter leur ratio coût-efficacité. Toutefois, c'est en investissant sur l'avenir que nous arriverons à convaincre l'ensemble des personnes de conserver et de redévelopper des services en France, avec en plus un enjeu de qualité. La souveraineté consiste aussi en le développement d'infrastructures de qualité.

Nous avons donc un gros travail à faire. Pour la fibre optique, nous sommes embarqués dans un chantier industriel hors-norme. Nous avons commencé avec du cuivre au début du XX^{e} siècle et il a fallu plusieurs dizaines d'années pour réaliser le réseau cuivre. Pour le réseau fibre, le programme a démarré à la fin des années 2000 et nous espérons avoir terminé la couverture d'ici 2025 ou peu après. Nous aurons donc créé en quinze ans une infrastructure énorme. C'est un chantier comme le pays n'en a jamais connu.

Nous avons de vrais sujets d'emploi et de qualité car, si le déploiement est rapide, il est parfois trop rapide. Même pour le cuivre, on voit encore en se promenant dans Paris des fils de cuivre sur les façades d'immeuble parce que, à un moment, il a fallu choisir de déployer très rapidement, les gens ne voulant pas attendre six mois. Actuellement, pour la fibre, vous n'attendez pas six mois mais quelques semaines avant d'être raccordé et, parfois, les déploiements vont très vite. L'enjeu de qualité est pour nous un enjeu de souveraineté pour disposer d'infrastructures pérennes à long terme.

Le soutien du Gouvernement et du Parlement est essentiel pour nous aider à faire émerger les services de demain, les emplois de demain et les industriels de demain. Le chantier de la fibre optique se terminera un jour. Il faut déjà réfléchir au développement suivant. Il portera notamment sur la 5G, sur les réseaux virtuels, les développements de logiciels, la maîtrise des données par les collectivités et plus globalement par les entreprises. Le soutien de l'État est essentiel sur ces sujets.

Nous travaillons avec l'État notamment dans le cadre du plan de relance. Nous avons avancé mais nous ne sommes pas encore au bout parce qu'il faut comprendre que, en investissant un peu maintenant, nous aurons un effet de levier énorme. Nous avions déjà eu cette discussion voici dix ans à propos de l'investissement dans la fibre optique. Lorsque nous avons présenté le premier plan fibre optique en demandant un programme de subventions notamment pour la fibre optique dans les zones rurales, tout le monde protestait. Dix ans plus tard, cela paraît naturel et le plan de relance a abondé le fonds pour permettre à la fibre optique de se développer plus loin dans les zones rurales.

Il faut discuter de ces questions pour refaire sur d'autres types de technologies et de services ce que nous avons fait sur la fibre optique voici dix ans. Nous en verrons le résultat

dans dix ans. Si nous n'avions pas fait ces choix, nous n'aurions pas aujourd'hui une des infrastructures en fibre optique les plus développées au monde.

L'enjeu de notre comité est de préparer les infrastructures de 2030. Le soutien public, des parlementaires et de l'État doit se faire maintenant. Dans dix ans, il sera trop tard. Nous avons des champions de la fibre optique en France. Cela doit nous permettre de développer des champions sur les autres domaines des infrastructures numériques de demain.

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». C'est un bon résumé des points de vue des différents groupes de travail et des différentes fédérations qui composent notre CSF.

Sur la partie fibre optique, la France met en œuvre actuellement un chantier formidable qui fera de notre pays le plus avancé d'Europe. L'infrastructure que nous construisons aura de nombreuses années d'avance sur l'ensemble de nos voisins, ce qui sera un accélérateur de transition formidable. Nous en avons bien besoin dans cette période de crise.

Pour nous, la souveraineté passe aussi par la qualité et la pérennité des réseaux. Une grande partie de nos communications et de nos télécommunications passe encore par le réseau cuivre parce que, dans les années 1970, à travers le plan Câble, des choix ont été faits pour construire un réseau de grande qualité, en privilégiant sa pérennité. L'industrie française en a bénéficié, par exemple ACOME mais aussi l'entreprise Câbles de Lyon, devenue depuis Alcatel Câbles puis Nexans. Le citoyen s'y retrouve puisque, pendant plus de cinquante ans, ces réseaux de communication ont rendu bien des services et ils fonctionnent encore aujourd'hui.

Sur la fibre optique, l'enjeu est similaire si ce n'est que nous construisons le réseau en un temps encore plus court. Les gouvernements se sont succédé en maintenant le cap, voire en accélérant ces dernières années, pour aboutir à un raccordement de l'ensemble de la population dans les délais les plus brefs, en amenant la fibre optique absolument partout et surtout dans les territoires. Ce sera un accélérateur de mutation économique.

La construction de ces réseaux dans les territoires passe par des réseaux d'initiative publique qui font appel à des délégations de service public, à des systèmes de sous-traitance. Nous avons alerté les pouvoirs publics sur l'importance de la qualité, de la pérennité, du respect des cahiers des charges, tant sur le choix des matériels que sur la mise en œuvre. Il s'agit de limiter la main-d'œuvre détachée, de limiter l'importance de produits exotiques qui ne respecteraient pas les règles de l'art, voire les règles du commerce international.

Nous avons de nombreux dossiers en cours pour attaquer au niveau européen des produits d'origine chinoise pour dumping. Le Gouvernement est intervenu pour sensibiliser les collectivités territoriales à l'absolue nécessité de respecter les cahiers des charges, de veiller à la qualité et à la pérennité des réseaux. Il faut mettre en place des contrôles puisque c'est de l'argent public qui est dépensé. Je souligne que, malgré ce plan massif de déploiement qui bénéficie à notre industrie, les trois plus belles usines européennes de fabrication de fibre optique, situées en France, sont toutes aujourd'hui en sous-activité, parce qu'elles subissent la concurrence asiatique qui ne respecte pas forcément les règles du marché ni les règles de la concurrence. Des questions se posent même souvent sur la qualité de ses produits. Il est important d'avoir le soutien du Gouvernement, des pouvoirs publics et des parlementaires pour sensibiliser les territoires sur ces points.

Le deuxième volet de la souveraineté concerne la sécurité. Le CSF « Infrastructures numériques » crée actuellement une passerelle avec l'autre comité stratégique de filière

mobilisé autour de la cybersécurité, qui rassemble aussi un grand nombre d'acteurs, champions français ou européens de ce secteur.

Mme Marie-Thérèse Blanot, déléguée générale du SYCABEL. Le déploiement de notre réseau très haut débit est un travail collectif. Dès le départ, des experts ont travaillé ensemble et avec l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) pour définir la façon dont nous posions et raccordions les câbles pour faire en sorte que ce réseau soit parfaitement adapté à nos besoins. Nous nous sommes projetés dans les besoins et les usages que nous aurions dans le futur.

Il faut insister sur ce travail collectif des donneurs d'ordres, de toutes les entreprises de la filière sur ces produits et leurs caractéristiques techniques. Nous avons par exemple défini tous ensemble quel type de fibre nous voulions utiliser pour le déploiement de ces réseaux très haut débit. Même si nous n'avons pas commencé par le très haut débit, nous avons dès le début réfléchi à ce que seraient les usages et les besoins, avec l'ensemble de la filière et des industriels. C'est pour cette raison que des investissements ont été faits au niveau de l'outil industriel pour les câbles ainsi que de la formation de toutes les entreprises amenées à utiliser, installer et raccorder ces câbles.

L'excellence de notre réseau numérique et de notre savoir-faire nous permettra d'être présents à l'export puisqu'il faut toujours penser au futur. Nous cherchons donc un étendard qui nous permettra de valoriser notre filière à l'international.

M. Philippe Latombe, rapporteur. Vous avez parlé des *smart cities*, de la 5G, des nouveaux réseaux. En tant que professionnels, comment percevez-vous la société sur ces sujets ? La France et les Français ont-ils une appétence pour ces développements ? Voyez-vous au contraire des résistances comme celles que nous avons vues pour la 5G ? Quelle vision en avez-vous ?

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». C'est une très bonne question d'autant plus que la covid et les nouvelles pratiques en termes d'usages ont eu aussi un impact significatif.

M. Michel Combot, délégué général du CSF. Nous ne sommes pas tout à fait en haut de la chaîne mais tout de même à un niveau où nous sommes énormément en contact avec les clients finaux, entreprises et particuliers. Nous avons d'ailleurs pu maintenir notre activité grâce à toute la filière : les opérateurs travaillent collectivement avec les installateurs, les fabricants.

Nos réseaux ont pu absorber des pics de trafic exceptionnels au soir du premier confinement. Nous ne nous attendions pas du tout à voir de tels pics de trafic, notamment sur le trafic voix : les gens ont commencé à rappeler leurs collègues ou leur famille par téléphone. Nous avons dû faire des adaptations car les usages ont complètement changé avec cette crise sanitaire. Malgré les enjeux de fracture numérique, les gens ont pu continuer à travailler, à s'éduquer. La fracture numérique porte sur l'accès et c'est pour cette raison que nous développons la fibre optique et la 4G actuellement, la 5G étant la technologie de demain. Nous avons besoin que l'ensemble des Français et des entreprises aient accès à cette technologie.

Des questions légitimes se posent sur les usages ; il ne faut pas faire n'importe quoi en profitant de la disponibilité de l'accès. Cette réflexion sur les usages n'est pas encore vraiment mûre, parfois encore assez caricaturale comme nous le voyons sur la 5G où le terme « amish » était à mon sens assez malheureux. L'idée n'est pas d'opposer mais de faire comprendre quel est l'intérêt de ces nouveaux services, de ces nouvelles technologies, ce qu'ils peuvent

apporter, y compris en matière environnementale. Le numérique serait un pollueur, une source de gaz à effet de serre. C'est vrai, comme pour toute technologie mais le numérique permet aussi des économies de gaz à effet de serre. Ainsi, le télétravail fait que les gens se déplacent beaucoup moins.

Il faut faire de la pédagogie. Nous avons été victimes de *fake news*. Des antennes ont brûlé et des infrastructures ont été dégradées. Les responsables sont des personnes qui surfent sur les rumeurs colportées notamment par les réseaux sociaux. Le débat est caricaturé pour des raisons politiques alors que notre filière ne fait pas de politique : elle développe des services, investit, crée de l'emploi et apporte des services demandés par les usagers.

Les gens nous demandent quand la 4G arrivera, quand la fibre arrivera et, maintenant, quand la 5G arrivera. Le besoin existe mais doit être maîtrisé. Ce n'est pas une fin en soi ; c'est un outil qui doit être au service d'un objectif. Nous devons être pédagogues comme nous l'avons été au début du confinement en demandant aux gens d'utiliser le wifi plutôt que le réseau 4G qui doit être réservé aux gens en mobilité. Nous avons aussi demandé aux gens de ne pas mettre des tunnels de vidéos qui surchargent les réseaux. Nous avons essayé d'être pédagogues sur le bon usage des réseaux comme avec les ampoules à basse consommation : ce n'est pas parce que l'ampoule consomme moins qu'il faut la laisser allumée toute la nuit. De même, ce n'est pas parce que le réseau est connecté en permanence qu'il faut forcément le charger car cela a un coût sociétal et qu'il existe également des enjeux de dépendance, notamment pour les jeunes.

Cette réflexion n'est pas simple car elle est souvent caricaturée, notamment pour des raisons politiques. Nous aimerions un débat sain, objectif, basé sur des études et traitant des vrais problèmes : les conseils aux parents dépassés par leurs enfants en matière d'usage du numérique, le conseil aux entreprises pour les convaincre de se numériser parce que c'est un enjeu essentiel, notamment durant cette crise sanitaire pour les commerces pour vendre, pour les entreprises pour être concurrentiels par rapport à leurs concurrents étrangers. Au-delà des grande déclarations, l'enjeu est de savoir comment être pédagogue, comment arriver à faire comprendre aux entrepreneurs et aux familles les enjeux du numérique, ce qu'il apporter de bien et de moins bien. Nous essayons de prendre part au débat, d'aller au-delà des *fake ne*ws et des caricatures.

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». Je salue d'ailleurs l'excellent travail réalisé par l'ensemble de notre filière. Du fait de la crise covid, nous avons considérablement modifié nos pratiques et donc les usages de nos infrastructures numériques. Il faut souligner que ces infrastructures ont très bien fonctionné, malgré l'impact de la covid. L'ensemble de la filière a pu agir pour maintenir en fonctionnement le réseau, assurer la qualité des transmissions. Des consignes ont été données, des actions spécifiques mises en place, avec même des mesures de soutien très significatives mises en place par l'ensemble des acteurs de la filière, des avances de trésorerie des grands opérateurs pour soutenir les fournisseurs en cascade. Si la crise covid a évidemment eu un impact sur les conditions de construction, d'installation, de mise en œuvre, l'ensemble de la filière est tout de même resté mobilisé pour assurer le bon fonctionnement.

Nous avons même fait une livraison d'une usine en Normandie lors de laquelle nous avons photographié un touret de câble de 1 000 paires de cuivre de 6 ou 7 tonnes, ce que nous n'avions pas fabriqué depuis des années. Il a fallu le fabriquer en urgence pour maintenir la qualité des anciens réseaux en place à base de cuivre. Il était hors de question que se produise une rupture de cet ancien réseau même si la technologie de demain est la fibre.

Le CSF entreprend des actions pour la mise en place des plateformes 5G mais aussi des actions à travers les territoires pour faire de la pédagogie, de la démonstration au niveau des collectivités territoriales en vue de mettre en place des infrastructures pour les territoires intelligents. Cela concerne souvent des quartiers, des collectivités.

M. Aubin Bernard, chargé de mission à InfraNum. Dans le cadre du projet structurant « *Smart* Territoires » appelé aussi « Territoires intelligents et connectés » qu'InfraNum copilote avec SYCABEL, l'idée est d'accompagner les collectivités dans leur projet de territoire connecté, de leur proposer des contenus pédagogiques pour les aider à comprendre les enjeux et les usages qui seront possibles dans le futur. Nous accompagnons aussi tous les industriels qui proposent des solutions aux projets des collectivités.

Dans le cadre du groupe de travail « *Smart* Territoires », nous avons plusieurs livrables en cours qui seront révélés d'ici la fin du mois. Une étude du Pôle interministériel de prospective et d'anticipation des mutations économiques (Pipame) a été lancée pour créer un cadre de compréhension des territoires connectés à la française, avoir une vision partagée et commune de ce que sont les territoires connectés en France et de ce vers quoi ils vont dans le cadre de ces projets.

Nous avons également une partie évènementielle dans laquelle nous faisons se rencontrer les collectivités et les industriels. Ainsi, à Angers, au mois de septembre, nous avons réuni 300 industriels et collectivités pour les faire échanger, notamment par l'intermédiaire d'ateliers participatifs, sur les sujets de la *Smart City* et tout ce qui y touche. Il s'agissait de voir les idées de chacun pour contribuer à avancer vers un cadre commun qui aboutira à une bonne prise en compte de ces projets par l'État. Nous espérons aussi un soutien financier aux projets des collectivités.

Mme Marie-Thérèse Blanot, déléguée générale du SYCABEL. Nous allons au plus près des besoins exprimés pour voir comment, à travers ces villes intelligentes, nous pouvons proposer un modèle. Il sera forcément différent entre les très grandes villes comme Paris ou Lyon et les plus petites villes ou même les villages dont les besoins sont très différents. Les solutions proposées doivent être adaptées et c'est un enjeu de formation et de compréhension qui peut être démultiplié par les collectivités, par les maires au niveau des usagers. Ce travail collectif d'explication et de formation est très important.

M. Michel Combot, délégué général du CSF. Le plan de relance a abondé les fonds destinés à la fibre optique ce qui est très bien, la crise nous ayant montré l'appétence de gens pour la fibre optique. Nous avons réussi à obtenir des enveloppes pour soutenir un certain nombre de projets structurants en matière de 5G et nous aimerions étendre ces appels, fléchés « souveraineté » d'ailleurs. Cela entre pleinement dans notre logique d'investir dans des projets qui doivent à notre pays de retrouver sa souveraineté, en termes de solutions, d'emplois, d'entreprises et de services.

Notre gros enjeu est de dupliquer ce que nous avons fait sur la 5G avec des projets liés aux territoires intelligents, aux territoires connectés pour soutenir des offres souveraines françaises pour le développement des services sur notre territoire, peut-être dans des domaines spécifiques. Cette offre française pourra ensuite s'exporter.

Les discussions sont en cours avec le Gouvernement. Nous pensons que l'investissement d'aujourd'hui prépare ce que sera la France dans dix ans. Il est normal que le plan de relance ait un effet à court terme, qu'il soutienne les entreprises pour passer cette crise économique sans précédent mais ce plan de relance doit aussi préparer ce que sera la France dans dix ans avec des investissements à moyen et long termes. L'idée est d'avoir un effet

d'entraînement pour que des plateformes voient le jour et fonctionnent pendant un temps de façon à ce que les gens comprennent quel est l'apport de ces services au niveau local, que des PME puissent développer leurs propres services. Ensuite, la filière prendra son envol.

Tout relais et tout appui des parlementaires dans ces discussions seront précieux pour aider le Gouvernement à faire ces arbitrages dans le plan de relance. Il faut garder un équilibre entre le court terme et le long terme mais aussi avec l'efficience même du plan de relance.

Par exemple, sur la 5G, nous devons faire un gros travail de pédagogie auprès des porteurs de projet pour qu'ils parviennent à franchir les barrières administratives liées au plan de relance. Lorsqu'il faut déposer un dossier à la Banque pour l'investissement (BPI), que l'instruction est ensuite faite par les services de l'État avant des arbitrages au Gouvernement, vous trouvez tout au long différents types de barrières. Nous avons donc décidé de faire des réunions une fois par semaine avec les différentes administrations pour comprendre où nous en sommes, voir les difficultés et accompagner les projets les uns après les autres.

C'est un gros travail avec le souci que le plan de relance ait à la fois un effet immédiat et un effet structurant pour le long terme. Au-delà des annonces et des chiffres, il faut que le plan de relance ait des effets concrets.

Ce n'est pas simple, notamment pour des petites PME, de remplir des dossiers. Nous avons ainsi vu un projet 5G porté par un institut d'enseignement et de recherche auquel était demandé un Kbis. L'institut avait du mal à expliquer à BPI France qu'il n'avait pas de Kbis parce qu'il s'agissait d'un projet de recherche et développement en matière de 5G qui devait amener à la structuration de briques essentielles.

Nous avons ces difficultés concrètes quotidiennement pour faire comprendre que le plan de relance doit préparer demain mais aussi être efficient. Si nous annonçons des chiffres sans que ces chiffres se traduisent en investissements, nous aurons raté une occasion alors que cette crise peut nous permettre de préparer l'avenir.

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». En tant qu'industriels de la filière, nous insistons sur le fait qu'il faut tout faire pour conserver une valeur ajoutée en France, dans nos territoires. Avons-nous identifié pour cela des mesures plus ciblées en termes d'impacts, de fiscalité ?

M. Michel Combot, délégué général du CSF. Les enjeux de fiscalité sont assez importants parce que nous tous ici payons des impôts en France et ce n'est pas simple de voir que d'autres disposent d'un cadre différent, aussi bien en ce qui concerne des produits importés que des services offerts aux Français. Nous avons à peu près gagné la bataille de l'opinion auprès du Gouvernement et de l'Europe mais nous ne sommes pas encore arrivés à des solutions suffisamment efficaces.

Un certain nombre de pays disposent de coûts et d'un environnement fiscal complètement différents, bénéficient d'aides d'État voire d'une fiscalité accommodante. C'est un véritable enjeu pour nos industriels. Nous devons pouvoir nous battre à armes égales. La crise économique est déjà compliquée mais si, de plus, d'autres pays jouent avec des règles différentes, nous ne pourrons pas, nous industriels, parvenir à développer ces éléments. Il s'agit de la taxe GAFA, de s'assurer que les conditions d'import-export soient les mêmes pour tous et que nous n'ayons pas une concurrence déloyale entre acteurs.

Je pense que c'est un enjeu important pour notre filière parce que des arbitrages de très court terme peuvent bénéficier à certains du fait que les coûts sont moindres mais, ensuite, la

qualité de service et la souveraineté sont en jeu. Nous bataillons pour nous assurer que le cadre soit propice à l'investissement en France et à la création d'emplois.

M. Philippe Latombe, rapporteur. J'aimerais avoir votre avis sur le rôle des collectivités locales. Comme vous l'avez dit, les collectivités locales sont plutôt acquises à l'idée de développer les réseaux et de pouvoir s'en servir parce qu'elles le voient comme un moyen de redynamiser le territoire. Dans les appels d'offre et les différentes discussions qui ont lieu avec les collectivités, avez-vous des points de friction, des points d'alerte ? Vous avez parlé d'un concurrent chinois qui intervient de façon un peu agressive sur les marchés. Comment cela se passe-t-il avec les collectivités territoriales lorsqu'elles ont ce type de projet et le mettent en pratique avec des appels d'offres ?

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». Il ne s'agissait pas d'un concurrent chinois mais de nombreux concurrents chinois ou asiatiques. Ils bénéficient de l'appel d'air du marché français qui est le marché occidental le plus dynamique aujourd'hui. Les acteurs de la filière veulent en tirer le maximum d'avantages pour défendre leur marge. La combinaison avec des sous-traitants en cascade nous a alertés sur deux points.

Le premier point, essentiel, est de savoir si ces réseaux construits dans des collectivités territoriales par l'intermédiaire de nombreux sous-traitants respectent bien les règles de l'art, les cahiers des charges et quelle sera la qualité du réseau ainsi construit. La vocation de ce réseau est de durer au moins une cinquantaine d'années. Nous avons alerté les autorités compétentes : les pouvoirs publics, l'autorité de régulation… Diverses actions ont été mises en œuvre et méritent, je pense, d'être poursuivies.

Le deuxième point qui est venu se greffer sur ce problème concerne des règles économiques qui n'étaient pas respectées ce qui a nécessité des actions au niveau européen. La France est engagée mais aussi des acteurs allemands, anglais, italiens et même des Américains qui possèdent des usines en Europe. Une plainte pour des actions de dumping a été déposée et jugée recevable auprès de la Commission à Bruxelles. Elle est en cours d'instruction et devrait aboutir dans les prochains mois.

La perception des collectivités territoriales est grandissante. En discutant avec les acteurs, les élus et les politiques des territoires, que ce soit dans les villes, dans les communes ou les communautés de communes, dans les départements, nous voyons que l'un des sujets qui suscite le plus d'intérêt dans la population est le raccordement à la fibre optique, le très haut débit.

En effet, un agriculteur dans une ferme a besoin de se connecter à internet et donc d'avoir du débit pour son métier de tous les jours, pas uniquement pour regarder la météo mais pour faire des projections, pour traiter avec ses fournisseurs, avec ses clients, pour échanger avec les coopératives… Les familles, les citoyens et même les personnes âgées ont besoin d'avoir du très haut débit, par exemple pour avoir leurs petits enfants chez eux pendant les vacances de Noël. Les exemples de ce type se multiplient pour montrer que le très haut débit prend tout son sens, surtout dans les territoires. Les citoyens sont très mobilisés.

Le territoire connecté est plus une décision qui relève du bien public et de son impact politique. Il s'agit d'avoir une démarche écoresponsable, de faire des économies d'énergie, de consommation, de régulation de trafic, de gestion des déchets, de traitement des ordures ménagères, d'éclairage de la commune. Le raccordement de ces infrastructures ou de ces services publics devient un rouage primordial. La sensibilité à ces sujets est relativement variable. Le politique doit-il se mobiliser, est-il sollicité par les citoyens ou au contraire veut-il impulser une réelle dynamique ? Certains territoires sont plus mobilisés car ils bénéficient

d'industriels locaux qui les sensibilisent, par exemple des fabricants d'équipements, des grandes implantations d'opérateurs ou des industriels acteurs du secteur. Certains politiques sont plutôt visionnaires, pensent que l'avenir va dans cette direction et veulent anticiper tandis que d'autres ont plus tendance à suivre le mouvement. En tout cas, le train est en marche.

Nous mettons différentes actions en place à travers le CSF avec des plateformes pour la 5G et une sensibilisation des territoires. Les actions du groupe « Emploi, gestion des compétences, formation » ont aussi un impact significatif.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder d'autres sujets ?

M. Jacques de Heere, vice-président du CSF « Infrastructures numériques ». Peut-être pourrions-nous aborder les travaux transversaux de la passerelle entre le CSF « Infrastructures numériques » et la sécurité.

M. Michel Combot, délégué général du CSF. Les enjeux de sécurité sont des enjeux naturels pour notre filière, d'autant plus que notre secteur est marqué par le phénomène de virtualisation. Ce terme de virtualisation désigne la part grandissante des logiciels dans la gestion des infrastructures. Nous avions voici vingt ou vingt-cinq ans un câble et un commutateur. Nous avons toujours un câble, qui est maintenant en fibre optique, mais nous avons aussi des ordinateurs, des logiciels, des antennes et donc de nombreux éléments d'équipement notamment de nature logicielle. Nous ne parlions voici vingt-cinq ans que de voix et peu de données. Maintenant, tout passe par internet, même la voix.

Ces enjeux de cybersécurité sont devenus très importants, vitaux pour nos infrastructures. La France dispose d'un des cadres les plus complets en matière de sécurité. D'une part, tous les opérateurs de télécommunications sont des opérateurs d'importance vitale et mettent en œuvre de la directive européenne *Network and Information Systems* (NIS) qui oblige à avoir un certain nombre de procédures pour éviter toute faille de sécurité dans le réseau. D'autre part, la collaboration est assez intense avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur tout ce qui concerne le design du réseau. Notamment, sur la 5G, nous travaillons depuis plus de deux ans avec l'ANSSI pour savoir comment les réseaux doivent être construits au niveau logiciel pour être les plus efficients du point de vue de la sécurité. La loi prévoit de regarder à la loupe tous les équipements mis dans les réseaux 5G. Elle a aussi mis en place un système de sondes qui permettent de détecter des cyberattaques sur nos réseaux.

Cette part grandissante du logiciel nous amènera à élargir un peu l'horizon de nos infrastructures. Il faut voir ensemble infrastructures et services numériques. La France dispose de compétences assez importantes dans le secteur du logiciel, avec de grands champions du développement et de l'intégration logicielle. Nous devons travailler avec eux, au sein de notre comité mais aussi avec le comité qui s'intéresse vraiment aux enjeux de sécurité. Nous souhaitons disposer d'une feuille de route commune, de projets communs pour nous assurer que l'ensemble des industriels vont dans la même direction.

C'est donc un sujet important car tout est internet, tout est numérique et, demain, tout sera logiciel. S'il était compliqué de « hacker » un commutateur télécom, pirater un ordinateur ou un système logiciel est devenu pas exactement à la portée de tout le monde mais certains pays sont des spécialistes. Comme nous l'allons vu avec Sopra Steria qui a fait l'objet d'une attaque massive avec du rançonnage, même les grosses entreprises et les gros fournisseurs ne sont pas à l'abri de cyberattaques. C'est un enjeu collectif. Il faut que nos infrastructures soient les plus résilientes et permettent de servir la défense des intérêts français en matière de cybersécurité.

Les technologies en elles-mêmes ne sont pas bonnes ou mauvaises ; ce sont des outils. Ce qui permet d'être plus efficace globalement ouvre aussi d'autres failles sur lesquelles il faut travailler. Notre enjeu en matière de cybersécurité porte sur la 5G et sur la partie territoires connectés. Qui dit numérisation des services publics dit aussi protection à mettre en œuvre. Il s'agit de protection physique puisque des câbles sont sectionnés, des antennes brûlées et il faut aussi développer une protection cyber de nos infrastructures. C'est pour nous une priorité, avec d'autres industriels et en coopération avec l'État.

Table ronde ouverte à la presse, consacrée aux collectivités territoriales, avec M. Ariel Turpin, délégué général de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA), Mme Valérie Nouvel, vice-présidente du département de la Manche, Mme Ann-Gaëlle Werner-Bernard, conseillère parlementaire de l'Assemblée des départements de France (ADF), M. Guilhem Denizot, conseiller innovation de l'ADF, et M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France

(10 décembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je suis très heureux de la présence des représentants de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA), de l'Association des départements de France (ADF) et de Régions de France.

Nous recevons M. Ariel Turpin, délégué général de l'AVICCA. L'ADF est représentée par Mme Valérie Nouvel, vice-présidente du département de la Manche, Mme Ann-Gaëlle Werner-Bernard, conseillère parlementaire de l'ADF et M. Guilhem Denizot, conseiller innovation de l'ADF. M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France, est également présent.

Le but de cette table ronde est de prendre connaissance de la façon dont les collectivités perçoivent la notion de souveraineté numérique nationale et européenne. Notre démarche entre dans le cadre de notre réflexion sur la souveraineté numérique. Les collectivités locales sont à la fois partenaires et porteuses de nombreux projets numériques. Elles participent à la commande publique, au soutien des acteurs économiques locaux. Elles sont aussi confrontées à la protection des données de nos concitoyens et à la nécessité de faciliter l'accès au numérique en partenariat avec l'État et les acteurs privés.

Notre objectif est de faire le lien entre les interrogations de notre mission sur la construction d'une souveraineté numérique à l'échelle nationale et européenne et les attentes et déclinaisons possibles dans les territoires.

M. Philippe Latombe, rapporteur. Je me réjouis que nous ayons l'occasion d'échanger avec les représentants des collectivités territoriales. Nous souhaitons vous entendre sur plusieurs sujets.

Je voudrais d'abord vous interroger sur le sens que revêt selon vous la notion la souveraineté numérique. C'est un concept, parfois rapproché de celui de l'autonomie, qui désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et à ne pas subir les contraintes imposées par certains acteurs publics comme les États ou privés comme les géants du Web (GAFAM). Quel regard portez-vous, en tant qu'acteurs publics, sur la montée en puissance de cette thématique ? De quelle façon cette notion pourrait-elle se traduire, à votre échelle, de façon opérationnelle ?

Ma deuxième interrogation porte sur vos attentes et vos besoins dans le domaine du numérique. Les collectivités sont mobilisées dans le cadre du déploiement des réseaux fixes et mobiles. Elles font face à une demande forte d'accès à une connexion de qualité mais doivent aussi prendre en compte les craintes des citoyens comme nous le voyons avec la 5G.

Les collectivités sont impliquées au sein d'un grand nombre de projets numériques de toutes natures et contribuent aussi comme acteurs de la commande publique. Je souhaite que nous fassions ensemble le point sur ces différents sujets sous le prisme de la souveraineté numérique française et européenne et en incluant l'enjeu du risque cyber qui s'est parfois matérialisé concrètement ces derniers mois pour les collectivités.

Enfin, la souveraineté numérique implique aussi que les entreprises s'approprient le numérique, ne dépendent pas nécessairement d'acteurs étrangers et restent concurrentielles. Les petites et moyennes entreprises et industries (PME et PMI) souffrent en France d'un taux de numérisation très bas, raison pour laquelle le plan de relance contient un important volet consacré à cette question. Vous qui êtes en lien avec les acteurs économiques locaux, comment percevez-vous cet enjeu avec les interlocuteurs qui représentent ces entreprises ?

M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France. Je suis le conseiller développement économique de Régions de France et en charge également du numérique. Nous travaillons régulièrement avec les collectivités et nous travaillons d'ailleurs de façon plus fluide horizontalement avec les collectivités que verticalement avec l'État.

Le numérique est une compétence très largement partagée par les collectivités. En fonction des compétences qui nous sont dévolues par le législateur et le code général des collectivités, nous avons des entrées variables sur le numérique. L'entrée se fait par les infrastructures, avec des compétences très partagées, et surtout par les usages. La question de la souveraineté est donc particulièrement importante pour nous.

Les régions sont le chef de file du développement économique depuis la loi NOTRe ; elles partagent cette compétence avec les communes et les établissements publics de coopération intercommunale (EPCI). Elles ont également des compétences en matière d'aménagement du territoire à travers les schémas régionaux d'aménagement et de développement durable du territoire (SRADDT). Elles sont gestionnaires des fonds européens. Notre entrée sur le numérique est donc multiple.

Les principaux chantiers sur lesquels nous sommes actuellement mobilisés concernent les infrastructures fixes avec le déploiement du très haut débit. Nous sommes aussi très intéressés par l'achèvement des réseaux d'initiative publique, avec en particulier des discussions entre l'État et les régions Auvergne-Rhône-Alpes et Bretagne. Les régions sont partenaires sur le mobile à des niveaux variables mais apportent un appui aux collectivités infrarégionales pour le déploiement.

Toutefois, ce qui de par nos compétences nous mobilise le plus aujourd'hui est la question des usages. Elle est liée aux enjeux de développement économique et de souveraineté que vous avez évoqués. Nous travaillons avec la filière et les opérateurs en réfléchissant sur les enjeux économiques, les enjeux industriels particulièrement dans le contexte de la relance. La numérisation des entreprises, la digitalisation des très petites entreprises (TPE) et des PME constituent un chantier majeur pour l'État, les collectivités et les régions. Nous travaillons avec l'État sur le dispositif France Num et sur les nombreux dispositifs déployés par les régions dans le cadre de plateformes de e-commerce ou de la mise en place du chèque numérique. Nous travaillons aussi autour des enjeux de l'industrie du futur.

Dans le cadre de ce travail partenarial, les enjeux de gouvernance du numérique nous paraissent très importants. C'est pour nous un angle mort du code général des collectivités territoriales.

Les enjeux de l'industrie du futur portent sur les 10 000 diagnostics déployés avec l'État, sur la stratégie de filière, sur l'intelligence artificielle, sur la cybersécurité et sur le numérique éducatif. Cette question a pris toute son importance dans la crise que nous traversons. C'est encore une compétence partagée, les régions intervenant sur les lycées, les équipements, l'acquisition et la maintenance des infrastructures.

La souveraineté numérique comporte bien sûr des enjeux de sécurité, de résilience, de maîtrise. Il s'agit d'enjeux d'intégration et de maîtrise des technologies, par nos acteurs économiques mais aussi par les administrations, par nos filières, par les citoyens. C'est un enjeu de résilience et de capacité de nos réseaux à supporter la charge. Nous avons bien vu au moment de la crise quels étaient les acteurs, les régions ou les départements qui étaient les plus résilients, notamment sur le très haut débit. C'est aussi un enjeu de protection des infrastructures et des données. Nous lions également à la souveraineté numérique des enjeux d'inclusion. Cela touche même directement à la question de l'intégration républicaine. Nous avons aussi des enjeux de structuration de filière et d'innovation.

En ce qui concerne l'international, le numérique comporte un enjeu de « *hard power* » qui est notre capacité à déployer des infrastructures résilientes et à être pionniers dans le développement de technologies nouvelles. Il comporte aussi un enjeu de « *soft power* » qui est la question de notre capacité à discuter, à imposer des taxes et une fiscalité aux GAFAM, à établir un dialogue équilibré avec les opérateurs.

La France n'est pas forcément au point sur la cybersécurité. L'enjeu n'est pas de se substituer à Kaspersky. Nous pouvons créer des leaders nationaux sur ces sujets et c'est l'objectif des stratégies de filière, du quatrième plan d'investissements d'avenir (PIA), des stratégies d'accélération dans le cadre des investissements d'avenir. Toutefois, l'important est la capacité à discuter avec les fournisseurs d'équipement et de matériel, la capacité à défendre nos intérêts, sans forcément maîtriser nous-mêmes les technologies.

La souveraineté numérique est donc un enjeu de développement économique, social et environnemental ainsi que de sécurité nationale face au risque croissant de contrôle de la vie privée. L'approche doit être intégrée et transverse, plus intégrée que l'approche trop éclatée que nous avons aujourd'hui. Les enjeux autour du déploiement de la 5G doivent nous inviter à nous organiser collectivement pour piloter et mettre en œuvre ces chantiers.

Mme Valérie Nouvel, vice-présidente du département de la Manche, représentante de l'Association des départements de France (ADF). Je vous remercie de vous investir sur ce chantier de la souveraineté numérique. Ce sujet préoccupe beaucoup les départements.

En matière de souveraineté numérique, la priorité absolue des départements est le déploiement des solutions mobiles. C'est pourquoi nous nous investissons aussi au sein du comité de concertation France Mobile dans le cadre du « New Deal mobile ». Sans solution mobile à disposition des Français sur l'ensemble du territoire, il n'est pas possible de déployer des solutions de souveraineté numérique. Pendant la crise, plus de 40 % des collégiens ont suivi leurs cours à partir de leur mobile. Le mobile est vraiment la solution de demain, le focus des départements.

Pourquoi nous concentrons-nous sur le mobile ? Les départements sont persuadés que le meilleur coffre-fort des données est l'usager lui-même, donc son mobile. Pour bâtir une solution de souveraineté numérique en France, il convient d'inverser la tendance qui consiste à stocker des données dans de gigantesques serveurs qui sont très loin de chez nous, trop loin

de chez nous, qui sont aussi très énergivores et de revenir à des solutions dont le déploiement est porté par les régions et les départements pour stocker la donnée dans les territoires.

Il s'agit de serveurs alimentés par exemple par des méthaniseurs sur les exploitations agricoles. Des start-up françaises s'investissent dans ce projet et les régions portent le déploiement de ces solutions de transition énergétique. Il peut aussi s'agir de serveurs alimentés par les toitures photovoltaïques de nos bâtiments publics. Le but est de retrouver une territorialisation du stockage des données.

Lorsque je vous disais que le mobile de l'usager pouvait devenir un coffre-fort, c'est aussi parce que nous avons en France la chance d'avoir au niveau du pôle de compétitivité TES en Normandie des entreprises qui développent des solutions dans lesquelles le stockage des données est fait sur le mobile de l'usager en interfaçant ce mobile avec les sites utilisateurs de données. Nous nous affranchissons ainsi des questions de cybersécurité.

Actuellement, lorsqu'un énorme *data center* est attaqué, cela peut bloquer tout un département. Si les données sont sur les mobiles, l'attaque peut bloquer un usager ou les usagers les uns après les autres mais cela prend plus de temps. Nous sommes beaucoup moins vulnérables.

En matière de souveraineté numérique, je souhaite vous citer un exemple qui doit vraiment nous inspirer. Malheureusement, les départements sont aujourd'hui les seuls à avoir perçu le côté génial d'une solution française nommée NexSIS. Il s'agit du système numérique déployé par l'Agence du numérique de la sécurité civile (ANSC) pour nos pompiers. NexSIS est une solution française, développée par l'État, qui a tous les atouts que nous recherchons pour une solution de souveraineté numérique. Les départements s'y intéressent fortement parce qu'ils gèrent les services départementaux d'incendie et de secours (SDIS) mais aussi parce que cette solution permet d'interfacer d'autres usages numériques. Au sein de la commission « Innovation et Numérique » de l'ADF dont je suis vice-présidente et avec les services de la direction de l'information légale et administrative (DILA) qui dépend du Premier ministre, nous travaillons sur les possibilités d'interfacer à NexSIS tout ce qui concerne les fiches sanitaires de liaison de nos collégiens.

Il s'agit donc d'applications consistant à partir d'une solution souveraine développée par l'État sur laquelle, au niveau du territoire, nous pourrons articuler un ensemble d'usages numériques tout en assurant une protection des données. Cette protection des données est aussi une question de confiance des usagers et cette confiance est une des clés de la réussite.

Vous nous avez interrogés sur nos difficultés. Le caillou financier du jour dans nos chaussures est la problématique du fonds de compensation pour la taxe sur la valeur ajoutée (FCTVA). Le FCTVA doit s'appliquer sur toutes les solutions numériques en nuage. Or, nous avons été avertis hier que le FCTVA ne concernera finalement que les solutions « logiciel en tant que service » (SaaS) alors que vous savez bien que nous avons des solutions « infrastructure en tant que service » (IaaS) qui permettent aux détenteurs de logiciels de louer des infrastructures pour héberger les offres SaaS. Il est urgent de considérer ces solutions numériques en nuage comme un tout et d'appliquer les règles de FCTVA qui sont un levier financier non négligeable pour les territoires.

Le projet d'identité numérique renforcée peut nous permettre d'être rapidement des champions en matière de souveraineté numérique, en conjuguant nos talents entre État et territoires. Ce projet peine à progresser au niveau français ; il est souvent perçu comme une charge par l'État, tandis que les départements le voient comme une recette. Ce projet conjugue en effet à merveille souveraineté numérique et inclusion numérique. Lancer ce chantier est

pour nous une priorité absolue. Les départements sont candidats pour expérimenter la solution sur les territoires. Nous avons proposé cet appui depuis maintenant plusieurs années mais nous n'avons toujours pas de réponse.

S'agissant de la gouvernance, je souligne que ce que nous vivons au sein des comités France Mobile et France Très Haut Débit est très positif. Petit à petit, nous progressons pour mieux intégrer nos retours d'expérience sur les territoires. Ces comités sont des lieux de coopérations essentiels. Les programmes de développement concerté de l'administration numérique territoriale (DCANT) sont d'autres lieux de coopération qui peuvent aussi être intéressants pour développer des solutions de souveraineté numérique.

Les départements ont souhaité la création d'un comité 5G pour tenir compte des bons retours d'expérience que nous avions dans nos coopérations sur le « New Deal » dans le cadre du déploiement de la 5G. Ce comité 5G s'est mis en place et je pense que c'est vraiment une chance pour progresser ensemble en matière de déploiement de solutions numériques. Il ne vous a pas échappé que le développement de la 5G s'appuie sur des plateformes « *edge* » qui se trouvent dans les territoires. La territorialisation des solutions numériques est donc déjà en route.

M. Ariel Turpin, délégué général de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA). Je me concentrerai sur les questions de souveraineté et de transformation du marché professionnel.

Nous travaillons d'abord sur l'obtention de la donnée. Ce n'est pas anecdotique car nombre de collectivités ont des délégations de service public, sur l'eau par exemple. Leurs délégataires gèrent et exploitent de nombreuses données. Quand l'acquisition de ces données est possible, elle est souvent payante car elle n'est pas dans le contrat de service public. La société privée prestataire a finalement plus d'informations sur les citoyens que n'en a la collectivité. Notre première couche est donc l'obtention de la donnée et l'obtention d'une donnée qui ne soit pas en silos, qui puisse être interconnectée avec des données sur la circulation, sur les déplacements, sur les transports…

Le deuxième point concerne le stockage et l'utilisation. Les questions de *cloud* souverain sont tout sauf une lubie. Je le vois d'ailleurs avec les réactions assez épidermiques de certains acteurs privés du *cloud*. Dès qu'une collectivité évoque la possibilité d'avoir son propre centre de données et se propose de le partager avec d'autres collectivités, elle subit tout de suite des charges dans la presse de la part de ces acteurs privés.

La volonté de voir où sont stockées ces données est de plus en plus forte. Cela peut être chez les utilisateurs ou dans des centres de données pour des raisons de sécurisation. Beaucoup de régions, de départements ou de grosses villes y réfléchissent et cherchent à partager ces structures.

Après le stockage, nous arrivons à l'utilisation. C'est souvent là que la question de la souveraineté est la plus problématique puisqu'il faut disposer d'outils souverains. Je ne connaissais pas le projet NexSIS et je remercie Mme Nouvel d'en avoir parlé. Je connaissais en revanche d'autres projets sur lesquels travaillent des collectivités et nous travaillons également sur d'autres dans le cadre du programme DCANT.

Le dernier point qui est apparu récemment, en 2019-2020, concerne le renouveau des groupements fermés d'utilisateurs (GFU). Les collectivités, en particulier les régions, s'étaient historiquement lancées dans les réseaux à fibre optique autour de GFU pour des mono-usages, notamment pour l'enseignement supérieur. Ces GFU sont ensuite devenus des réseaux

d'initiative privée (RIP) lorsqu'il a fallu mutualiser. Beaucoup de gens pensaient que, avec l'arrivée massive de la fibre optique grand public, ces réseaux disparaîtraient mais nous constatons l'inverse. De plus en plus de collectivités souhaitent se réapproprier ces réseaux pour être maîtres de ce qui circule dedans, de la manière dont elles le font circuler et de la manière dont elles le sécurisent.

Par exemple, si un département ou une grosse commune ayant plusieurs sites à gérer passe par un prestataire de télécommunication qu'il ne connaît pas vraiment, qui a peut-être des actionnaires étrangers, qui utilise ses outils de protection et stocke de différentes manières, il faudra gérer autant de points de connexion que de sites, qui sont autant de points à sécuriser et à superviser. Beaucoup de collectivités avaient donc historiquement conçu des réseaux GFU dans des logiques d'économies mais nous voyons aujourd'hui apparaître des GFU sécurisés. Tout transite ainsi par la direction des systèmes d'information (DSI) d'une grosse collectivité, par des liens propres, plutôt que d'avoir à gérer plein de sites diffus. La DSI active elle-même le service, met tout en place et, entre le bâtiment et la DSI, il n'existe aucune sortie. Toutes les sorties se font au niveau de la DSI ce qui permet de concentrer la sécurisation et les sauvegardes en un seul point.

Ce phénomène s'accélère même dans certains territoires qui avaient abandonné cette logique. Par exemple, les Hauts-de-Seine avaient revendu tous leurs réseaux *fiber to the home* (FttH), *fiber to the office* (FttO). Ils reconstruisent aujourd'hui un réseau propre pour maîtriser l'intégralité de la chaîne, avec derrière les questions du stockage de la donnée, des redondances. En gérant toute la donnée de tout un territoire se pose la question de l'opportunité d'avoir son propre centre de données.

Sébastien Soriano, le président de l'Autorité de régulation des communications électroniques et des postes (ARCEP), soulignait que, depuis quinze ans, les réseaux d'initiative publique sont la seule preuve tangible de succès de cette transformation du marché professionnel. C'est pour nous un motif de satisfaction, mais très relatif au sens où cela ne concerne que très peu de territoires et un nombre marginal d'entreprises.

L'AVICCA et ses adhérents s'investissent donc aussi beaucoup dans des solutions plus générales comme celle de Kosc Télécom que nous avons soutenue dans toutes ses péripéties ces dernières années. Ils ont un modèle très proche de celui des réseaux d'initiative publique qui permet vraiment la transformation. Si vous ne changez pas de connexion, ce qui est difficile, si vous n'avez le déclic de changer d'opérateur et de partir vers un opérateur qui connaît bien votre marché, votre filière, votre fonctionnement, vous restez dans une sorte de ronronnement de confort, vous ne vous développez pas, vous ne vous numérisez pas et vous ne changez pas vos pratiques. Je parle de manière générale de l'économie, y compris des commerçants et des artisans, pas seulement des grandes entreprises et du secteur *high tech*.

Ainsi, hier, j'ai discuté avec mon coiffeur qui n'accepte toujours pas les paiements sans contact. Il m'a expliqué qu'il le fera l'année prochaine mais qu'il faut pour cela qu'il change de banque, d'opérateur, afin que les clients puissent payer avec leur téléphone mobile. Imaginez l'effort à faire pour changer de système !

Ce changement est difficile pour tout le monde, pour les particuliers lorsqu'il faut changer d'opérateur et pour les entreprises aussi. Plus les entreprises sont de petite taille, plus il est difficile d'évoluer. L'oligopole qui tient le marché n'a évidemment pas trop envie de changer les choses. On ne réveille pas un client qui dort ; c'est une devise du marché des télécoms. Nous essayons de réveiller tout le monde, nous secouons régulièrement ce marché. Nous sommes aussi derrière nombre d'actions pédagogiques.

Pour finir, un point du plan de relance nous embête beaucoup. Nous sommes très satisfaits du volet sur la transformation-numérisation des entreprises et des collectivités. Toutefois, sans connexion, cela ne sert à rien. Si nous ne prenons pas en compte cette rupture en termes de connexion, toutes les animations pédagogiques sur le terrain ne serviront à rien et nous gaspillerons de l'énergie, de l'argent. Connectons nos entreprises et nos activités comme nous le faisons pour nos administrations sinon nous allons droit à l'échec et nous rendrons moins efficient l'argent public investi dans le reste du plan de relance.

M. Philippe Latombe, rapporteur. Je reviens sur la 5G. Nous avons un grand plan de développement sur la partie télécom car peu de pylônes ont été installés en zone blanche depuis quinze ans et nous prévoyons d'accélérer. Nous sentons une réticence de certains de nos concitoyens sur la 5G. Comment le ressentez-vous sur le terrain ? D'où provient cette inquiétude ou cette réticence ? Comment la vaincre et développer le plus vite possible le réseau 5G ? Comment avoir une couverture aussi exhaustive que possible du territoire ?

Mme Valérie Nouvel, vice-présidente du département de la Manche, représentante de l'ADF. Il faut d'abord expliquer à nos concitoyens que la 5G n'est pas une évolution de la 4G sinon il est difficile de dire à des habitants qui n'ont pas encore accès à une connexion satisfaisante en 4G que nous voulons déployer la 5G. En expliquant aux gens que la 5G n'est pas une évolution de la 4G mais qu'elle permet par exemple de faire de la télémédecine, elle les concerne directement. Ils en voient mieux l'utilité en comprenant que la 5G permet d'échanger des données entre le médecin à la campagne et l'hôpital.

Il faut donc d'abord informer sur les usages et Cédric O vient d'ailleurs de nous envoyer des supports pour communiquer sur ce qui peut être fait avec la 5G. C'est un point essentiel qui lèvera déjà une difficulté.

L'autre difficulté, abordée par l'Association des maires de France lors du dernier comité 5G, est le fameux dossier d'information des maires. Il est urgent de bien le travailler car c'est le maire de la commune qui sera en première ligne face aux demandes des usagers et aussi d'associations qui sont contre la 5G. Si le maire est démuni dans sa mairie, incapable de donner des informations concrètes sur ce qu'il se passera sur le territoire, nous aurons dès le départ un blocage et des difficultés. Lorsque le dossier d'information contient uniquement un feuillet qui vient modifier un dossier datant de quinze ans pas forcément bien archivé en mairie, c'est compliqué.

Les deux points essentiels sont donc d'expliquer les applications aux usagers et de doter les maires des communes de l'ensemble des éléments nécessaires pour qu'ils puissent dire ce qu'il se passera sur le territoire.

Même si le déploiement de la 5G n'est pas administré comme le « New Deal », le comité 5G doit permettre d'avoir ce dialogue permanent entre collectivités et territoires pour que tout se passe bien.

M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France. Un élément d'explication des inquiétudes sur le 5G est la vision trop techniciste que nous avons depuis plusieurs années. Les enjeux d'infrastructures sont évidemment très importants mais les enjeux d'usages et de services numériques à la population ont été beaucoup moins pris en charge jusqu'à récemment. L'importance des usages est probablement un enseignement de la crise que nous voyons d'ailleurs apparaître dans votre saisine et dans la brochure diffusée par Cédric O, sur laquelle toutes les associations de collectivités ont travaillé.

Cette vision centrée sur la technique et les infrastructures nous semble restrictive. Au sortir de cette crise, quelques constats sont importants dans le domaine de la souveraineté numérique. Le « New Deal mobile » et le plan France Très Haut Débit sont globalement un succès mais nous ne pouvons pas ignorer qu'il reste des problèmes de connexion, que l'inachèvement de la couverture numérique fixe et mobile produit des inégalités dans l'accès au numérique. Le plan de relance devrait contribuer à réaliser ces raccordements plus compliqués.

Toutefois, la fracture numérique n'est pas simplement liée à la connexion mais aussi à la capacité à utiliser ces technologies. La manque de maîtrise des technologies par les acteurs économiques, les administrations et les citoyens est un facteur aggravant des inégalités ainsi qu'un facteur de déstabilisation pour la souveraineté ou la sécurité économique.

Les enjeux portent aussi sur la faible digitalisation des TPE et PME. J'alerte la représentation nationale sur la nécessité, dans le plan de relance, de mutualiser et d'articuler au mieux nos interventions. Par exemple, Alain Griset, ministre délégué auprès de Bruno Le Maire, a décidé le lancement d'un dispositif de chèque numérique de 500 euros pour les TPE. Or, les collectivités et les régions en tête sur ce sujet qui fait partie de leurs compétences disposent à peu près toutes, depuis plusieurs années, de chèques numériques, de dispositifs de soutien à l'équipement, à la formation, de diagnostics, de conseil pour des montants bien plus importants, qui peuvent aller jusqu'à 5 000 ou 6 000 euros. Nous avons alerté sur ce point, nous nous sommes difficilement fait entendre. Finalement, à notre grand désarroi puisque nous avions perdu pas mal de temps, dans le cadre du conseil économique État-régions mis en place voici un peu plus d'un an, le ministre a lui-même tapé du poing sur la table en disant que, dans l'intérêt des entreprises, il était inadmissible que nous multipliions les guichets et ne mutualisions pas mieux avec les dispositifs régionaux sur la digitalisation des TPE.

L'efficacité de nos actions est un enjeu très concret, qui suppose d'abord de se mettre à la place de l'usager. Il ne faut pas simplement penser à la technique. La maîtrise du e-commerce par un commerçant ou un artisan n'est pas uniquement un enjeu d'achat de matériel mais d'autonomisation. L'initiative des ambassadeurs est de ce point de vue une bonne initiative mais pensons aussi la question des usages, des services, la manière dont nous pouvons articuler nos interventions sur ces sujets.

En ce qui concerne les inquiétudes des citoyens, nous pouvons parler davantage de la qualité de vie, du service plutôt que de dire simplement que la 5G améliore les capacités de *streaming* ou apporte des potentialités plus importantes pour les joueurs en ligne. La 5G est utile à l'industrie, à la santé, pour la gestion optimale des ressources énergétiques. Nous avons essayé d'illustrer ces aspects dans la brochure. En insistant davantage sur ces enjeux d'usages, de services, d'amélioration de la qualité de vie, en prenant une approche moins techniciste, les craintes seraient sans doute moins grandes.

M. Ariel Turpin, délégué général de l'AVICCA. Le problème de communication sur la 5G est en cours de règlement puisque tous se mettent à faire de la pédagogie. C'est très bien et nous soutenons à fond ces actions essentielles.

Cela dit, l'ARCEP avait publié dès 2017 un livre blanc de la 5G. Des consultations avaient été faites mais avaient obtenu très peu de réponses. La communication a ensuite été assez maladroite, avec une approche assez techniciste. Je me souviens d'un propos très maladroit du président de l'ARCEP qui disait que la 5G sera moins nocive que la 4G grâce au *beamforming*, le filtrage spatial mais cela sous-entendait que la 4G est nocive.

Nous avons aussi un problème de calendrier avec les décisions de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) que nous n'avons pas encore sur la bande des 26 gigahertz. Tout ceci crée une atmosphère qui permet à certaines actions locales de prendre corps et forme de manière assez virulente. Nous observons que l'opposition se situe plutôt dans les villes, tandis que les destructions sont plutôt dans les campagnes. Ce sont donc ceux qui en ont le plus besoin et qui ne sont pas forcément les plus opposés qui sont les premières victimes. Lorsqu'une antenne saute en ville, d'autres prennent le relais tandis que, à la campagne, ce sont souvent plusieurs villages qui sont ainsi mis dans le noir.

L'arrivée de la 5G a un impact négatif sur le déploiement du « New Deal » et de la 4G. En effet, même lorsque les élus et les habitants étaient très favorables à l'arrivée de la 4G, nous constatons une réactivation des oppositions et des associations locales qui rend compliqué même le développement de la 4G. Nous avons donc une relative opposition entre ceux qui ont absolument besoin d'avoir une couverture mobile et ceux qui veulent à tout prix la refuser.

L'AVICCA ne se positionne pas sur le sujet des ondes, d'abord parce que la bande des 3,5 gigahertz qui vient d'être attribuée était la bande des collectivités. Nous avons été proprement – ce n'est pas péjoratif – expropriés de cette bande de fréquences par l'ARCEP, avec les délais utiles, des moyens financiers pour migrer vers d'autres fréquences. Cette bande n'est pas devenue nocive du fait de ne plus être confiée aux opérateurs publics et d'être confiée aux opérateurs privés. Nous ne parlons donc pas de la partie ondes.

Nous travaillons plutôt avec nos adhérents sur la pédagogie concernant les usages de la 5G, sur le déploiement équilibré entre zones rurales et urbaines. Si cette technologie n'est qu'urbaine, les gens verront se réactiver le spectre de l'absence de couverture 4G. Aujourd'hui, nous avons des oppositions et, demain, nous verrons des manifestations parce que la 5G n'est toujours pas arrivée, que c'est un scandale, que le maire et le conseiller départemental ne font rien, que nous ne nous occupons que des villes…

Nous étudions aussi l'impact environnemental, la consommation. Nous nous interrogeons pour savoir s'il faut arrêter certaines bandes de fréquences, s'il faut migrer en 5G certaines bandes actuellement utilisées en 3G. Je ne parle pas d'arrêter la technologie mais d'arrêter certaines bandes de fréquences à cause d'un rapport entre le nombre de gigabits transportés et la consommation énergétique très variable d'une technologie à l'autre.

L'intégration paysagère est un autre point très important, qui désamorce beaucoup de crises. Elle explique peut-être le fait que les gens se plaignent de la 5G dans les villes mais que les pylônes soient attaqués à la campagne. À la campagne, les pylônes sont visibles puisque ce sont des pylônes à treillis de 35 ou 40 mètres, bien visibles à des kilomètres à la ronde. Ils sont invisibles en ville puisque ce sont des fausses cheminées ou qu'ils sont sur des façades ou sur du mobilier urbain. La 5G sera très discrète et il se peut qu'elle soit parfois démolie sans le faire exprès.

L'intégration paysagère est à mon avis une approche essentielle. Nous avons des exemples de villes ou villages dans lesquels sont installées des *small cells*, des petites antennes positionnées sur le toit d'un bâtiment, mairie ou autre. Ces antennes fournissent une très bonne couverture. Il faut quatre ou cinq petites antennes de ce type à la place d'un gros pylône. Cela « passe comme une lettre à la poste », surtout si le maire a un dossier d'information mairie (DIM). Le DIM est un point essentiel, la première brique pour désamorcer énormément de conflits, pour que les gens n'aient pas l'impression que nous agissons en cachette.

L'intégration paysagère est importante car des antennes invisibles ou très discrète ne poseront pas de problème tandis qu'un pylône de 35 ou 40 mètres installé près d'un endroit que les gens apprécient beaucoup, où ils passent tous les jours, déplaira forcément. Dans ce cas, plutôt que l'esthétique, le meilleur moyen de fédérer les oppositions est d'insister sur l'émission d'ondes, les dangers sanitaires et cela peut provoquer encore plus d'oppositions.

M. Éric Bothorel. Les débats de ce matin sont très larges, sur des sujets parfois propres à notre pays. Les réactions sont plutôt rurales effectivement mais l'extrême gauche ne prendra pas le risque de détruire des stations radioélectriques en pleine ville alors qu'elle peut le faire assez sereinement à la campagne. Cela ne concerne d'ailleurs pas que l'extrême gauche puisque nous voyons aussi de pauvres hères qui ont voulu passer à l'action directe parmi ceux qui sont traduits devant les tribunaux depuis la cinquantaine de faits – destruction d'antennes ou camionnettes d'installateurs vandalisées – qui ont été commis au printemps.

Les *small cells* sont pratiques effectivement mais, en même temps, l'Agence nationale des fréquences (ANFR) se plaint de l'absence de DIM pour les *small cells*. Nous serons obligés de mettre un grand nombre de *small cells* puisque, plus la fréquence est élevée, plus la pénétration des ondes dans les bâtiments est faible. La couverture en milieu urbain sera donc probablement composée de centaines de *small cells* et il sera compliqué de déposer un DIM pour chacune de ces antennes. Il faut trouver un système qui permette à l'ANFR d'exercer ses missions de contrôle. L'ANFR rend d'ailleurs publics depuis quelques jours ces contrôles, avec une plateforme qui permet de consulter les niveaux d'émission sur les quelques éléments installés, à Paris déjà et bientôt à Rennes.

Je pense que la représentation nationale sera tout à fait d'accord avec la nécessité de mettre de la transparence tout en étant très pratique et en ne perdant pas de vue les progrès apportés par le « New Deal » qui a divisé par deux les délais d'instruction pour l'implantation des stations radioélectriques. En 2018, nous étions deux fois plus lents que le Royaume-Uni ou les pays du nord de l'Europe et c'est en partie la raison pour laquelle notre couverture mobile n'était pas à la hauteur. 600 pylônes ont été déployés en zone blanche depuis quinze ans, 2 000 seront déployés dans les deux ans qui viennent. Nous voyons bien l'accélération et il faut continuer ainsi.

La menace cyber plane aussi sur les collectivités. La cybercriminalité exerce aujourd'hui une pression extrêmement forte, sans précédent. Guillaume Poupard m'a dit : « *Nous sommes face à un mouvement exponentiel, nous sommes au début de la courbe et les attaquants ont de l'avance.* » Ce n'est pas souvent que le patron de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) révèle que groupes de presse, collectivités, TPE et PME, de manière non ciblée mais parce qu'il existe une opportunité, sont attaqués par des entreprises criminelles, notamment à partir des rançongiciels. Les collectivités ont dû, comme le reste de l'économie, inventer des dispositifs pour ouvrir des portes et permettre à un certain nombre de leurs agents de travailler en externe.

J'aimerais savoir ce que font les collectivités pour s'assurer que les prestataires qu'elles enrôlent sont de bon niveau, pour tester leurs systèmes. En effet, que peut-on imaginer d'autonomie stratégique ou de souveraineté si, par ailleurs, nos infrastructures sont fragiles ? Les collectivités privilégient-elles l'*open source* pour pouvoir tester ? Font-elles appel à des *bug bounty*, des primes aux bogues ? Quels sont les mécanismes mis en œuvre par les collectivités pour continuer à déployer des infrastructures tout en s'assurant qu'elles ne seront pas demain une cible pour cette menace, comme elles le sont déjà ?

Vous avez évoqué la mobilisation des régions pour la digitalisation des TPE-PME. Certes, de nombreux mécanismes existent. Vous n'avez pas évoqué celui de la banque des

territoires qui existe depuis le 1er mars à destination des communes, agglomérations ou organisations commerçantes et qui a été faiblement mobilisé. Dans ma circonscription des Côtes-d'Armor, pas une commune n'a mobilisé cette possibilité d'accéder à 12 000 euros pour connaître les flux de piétons, pour mettre en place un shopping de commune… Je ne peux pas imaginer que les actions n'ont pas été entreprises parce qu'il existe trop de dispositifs. Je voudrais savoir en quoi les dispositifs d'aide ont permis aux entreprises de se numériser. Avez-vous un bilan ?

Sur la partie FCTVA, dont je suis en partie responsable, il n'existe aujourd'hui parfois pas d'autres solution que d'avoir des logiciels en mode SaaS. Si nous avions enrôlé le mode SaaS, nous aurions créé un effet d'aubaine parce que le Saas existe déjà dans les collectivités alors que le IaaS est très peu présent. L'enjeu est de basculer sur des infrastructures IaaS ; le sujet est la « cloudification » des services des collectivités. Pardonnez-moi de ne pas avoir poussé en première lecture à l'Assemblée nationale un amendement qui aurait couvert les modes SaaS et *Platform as a service* (PaaS). Ces modes sont déjà assez massivement développés dans les collectivités et c'est le mode IaaS qui manque cruellement.

M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France. En 1997, les spécialistes de la sécurité nous disaient qu'environ 40 virus par jour étaient identifiés et traités. En 2017, nous en étions à 430 000 virus par jour. La cybersécurité est donc un enjeu majeur et, vous avez raison, la courbe est exponentielle.

Des régions ont vécu de façon très concrète ces attaques. Au mois de mars, une attaque qui a duré plusieurs jours a visé le conseil régional Grand Est. Rappelons également les difficultés qui ont touché en pleine pandémie le centre hospitalier universitaire (CHU) de Rouen.

Nous travaillons étroitement avec la filière aéronautique et le Groupement des industries françaises aéronautiques et spatiales (GIFAS), ce qui nous a permis d'être alertés juste avant la pandémie. Concrètement, la cybersécurité n'est pas uniquement l'usage de rançongiciels par des groupes mafieux mais ce sont aussi des enjeux souverains, avec souvent des groupes souverains.

Nous savons, pour avoir échangé avec les services de Bercy – Bruno Le Maire l'avait évoqué lors d'une rencontre avec les présidents de régions – qu'une recrudescence d'attaques a touché la filière sous-traitante d'Airbus lorsque Boeing a rencontré des difficultés sur son 737 Max. Nous en avions d'ailleurs aussi eu des retours sur le terrain. La volonté de rétablir l'équilibre ou, du moins, d'entraver d'Airbus alors que son principal concurrent, Boeing, était en difficulté, était claire.

C'est donc pour nous un sujet majeur, sur lequel il doit exister une stratégie nationale concertée, coconstruite avec l'État, les collectivités, les opérateurs. Il faut que tous les acteurs travaillent ensemble. Je me permets de soulever ce point car plusieurs acteurs majeurs sur le sujet de la cybersécurité nous signalaient s'étonner que le groupement d'intérêt public d'actions contre la cybermalveillance (GIP ACYMA) et l'ANSSI ne travaillent pas de façon évidente ensemble. Peut-être pourrions-nous déjà mieux articuler ces interventions.

Concrètement, c'est pour plusieurs régions un sujet clé dans leurs stratégies de développement économique et de soutien aux filières. C'est le cas dans le sud, dans le Grand Est, en Ile-de-France où sont clairement identifiés comme des axes forts les enjeux cyber et intelligence artificielle (IA). Nous travaillons sur ces enjeux avec les entreprises à travers de nombreux dispositifs. J'évoquais les 10 000 accompagnements à la maturité numérique des entreprises. Nous avons proposé, en obtenant une convergence de vues assez immédiate de

nos collègues de la direction générale des entreprises (DGE) de Bercy, que les 10 000 accompagnements lancés dans le cadre des dispositifs « Industrie du futur » puissent tirer les enseignements de la crise, et notamment que le volet cyber soit renforcé. Nous travaillons avec le GIFAS, y compris sur la cybersécurité.

La question est, vous avez raison, de mesurer l'effet de ces dispositifs. Le dispositif des 10 000 accompagnements fonctionne. Il aurait besoin sans doute d'être plus dynamique. Je me permets d'attirer, monsieur le député, votre attention sur un point, sans volonté de polémique inutile sur ces questions où nous devons agir collectivement. Nous avons une mauvaise tendance en France à doublonner les dispositifs. C'est très français, au grand dam d'ailleurs de ceux qui sont à l'intersection de nos actions.

Je prends le cas des consulaires, les chambres de commerce et d'industrie (CCI) et les chambres de métiers et de l'artisanat (CMA) qui sont mobilisées sur le chèque numérique, le seront demain sur du diagnostic, sur des formations et actions. Nous avons de l'autre côté des collectivités qui mettent en place leurs propres dispositifs. Dans le contexte budgétaire actuel des CCI, les organismes consulaires sont ravis de pouvoir émarger à ces différents dispositifs mais, en termes de mutualisation et de coordination de nos actions, ce n'est pas très efficace.

La question de l'optimisation de nos interventions, de notre capacité à faire levier sur nos dispositifs est une véritable inquiétude. Nous craignons que les ministères, bénéficiant de la manne sans précédent du plan de relance – 100 milliards d'euros – avec la contrainte de consommer cette somme dans les deux ans, de déployer rapidement, aient la tentation de fonctionner en silos plutôt qu'en interministériel. Ils s'appuient de plus sur des services en région qui ont été fortement réduits. Les directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi (Direccte) n'ont plus la capacité d'assurer ce rôle de relais. Les CCI ne peuvent pas être un substitut de notre point de vue et, d'ailleurs, je ne crois pas que la DGE le prévoie. J'insiste donc sur l'importance de réfléchir à nos modes de gouvernance, à la manière dont nous articulons les acteurs, y compris sur cet enjeu de cybersécurité.

Pour une action très concrète, nous avons signé en décembre 2019 avec le ministère de l'intérieur et avec Bercy une charte État-régions sur l'intelligence économique territoriale et la sécurité économique. Elle doit s'appuyer sur des comités régionaux à l'intelligence économique. C'est pour nous un outil important.

Nous avons le 30 novembre 2020 identifié avec M. Le Maire deux enjeux très forts sur les questions de cybersécurité. Le premier concerne la sécurité des écosystèmes de recherche et d'innovation car nous avons constaté une recrudescence des attaques sur les laboratoires de recherche, publics et privés. Le ministère de la recherche labellise actuellement des centres de données pour l'enseignement supérieur et la recherche dans chaque région. Il me semble que cet enjeu de cybersécurité n'est pas suffisamment pris en compte. La sécurité des écosystèmes d'enseignement supérieur et de recherche, la protection de la donnée, y compris dans les universités, est donc un sujet majeur. Il faut embarquer la communauté universitaire et les chercheurs sur ce sujet.

Le deuxième concerne la cybersécurité des entreprises, notamment des petites TPE, en jouant sur la proximité et la complémentarité de nos actions.

M. Éric Bothorel. Avons-nous des données sur le bilan des actions des conseils régionaux en faveur des TPE et PME ?

M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France. Nous pourrons fournir des chiffres à la mission mais je ne dispose pas de données dans l'immédiat. Nous sommes aussi comptables, autant que l'État et les différents acteurs, du faible niveau de digitalisation des entreprises. Moins de 40 % des TPE déclarent aujourd'hui avoir engagé une démarche de digitalisation mais une très forte accélération a eu lieu ces dernières années et ces derniers mois.

Nous avons lancé avec l'État le dispositif France Num en 2018, le dispositif 10 000 diagnostics dans le cadre de l'industrie du futur et nous travaillons à articuler nos actions dans le cadre de la relance. Vous avez raison quant au fait qu'il faut un bilan plus précis sur ces points.

M. Philippe Latombe, rapporteur. Nous serons preneurs si vous avez des chiffres.

Mme Valérie Nouvel, vice-présidente du département de la Manche, représentante de l'ADF. Au niveau des départements, en ce qui concerne la cybersécurité, nous pensons avant tout à la prévention des risques. Deux points nous préoccupent. Sur la partie infrastructures, les RIP ont l'avantage de permettre de disposer d'un réseau que nous maîtrisons, en particulier dont nous maîtrisons la qualité. Les départements coopèrent actuellement avec la mission Très Haut Débit sur l'aspect construction et pérennité des RIP.

Pensons également à nos collèges du point de vue de la sécurité. La Poste et la Caisse des dépôts et consignations ont pris le contrôle de Pronote. Certes, cela permet de conserver une certaine souveraineté mais nous attendions l'État sur ce point : qu'existe-t-il de plus intéressant en matière de souveraineté numérique qu'un outil comme Pronote ? Cela permettrait la protection des enfants, de leurs familles et des enseignants. Cela faciliterait aussi les retours d'expérience et les actions en matière de numérique entre l'État et les collectivités. La cybersécurité se gère à travers ce type d'action sur des infrastructures et des problématiques comme Pronote.

M. Ariel Turpin, délégué général de l'AVICCA. Je serais ravi d'échanger avec vous, monsieur Bothorel, sur le sujet des *small cells*. En Angleterre et en Allemagne, l'intégration paysagère est bonne. Même au bord des autoroutes anglaises qui ne sont pas des merveilles, vous ne voyez les pylônes qu'au dernier moment car ils ne dépassent pas au-dessus des arbres.

J'ai répondu en partie sur la cybersécurité lorsque j'ai dit que les collectivités cherchent à limiter le nombre de sorties vers internet. Lorsqu'une collectivité a énormément de sites, comme c'est souvent le cas des départements avec les SDIS et les collèges, le premier objectif est de minimiser les points de faiblesse. Cela ne pare pas tous les risques mais permet de mieux de mieux concentrer les actions sur un seul point plutôt qu'une multitude.

L'AVICCA assure aussi le partage d'expériences : ceux qui ont été attaqués disent pourquoi ils ont été attaqués, comment ils ont récupéré et comment ils se protègent désormais. Nous avons donc des tables rondes sur cette thématique de la cybersécurité. La dernière a eu lieu le 27 novembre ; le GIP ACYMA, la banque des territoires et l'ANSSI sont venus nous présenter les différentes démarches. Nous n'avons jamais 100 % des élus et des techniciens présents mais, à chaque fois, une cinquantaine de collectivités viennent s'acculturer. C'est un sujet très prégnant et l'AVICCA intègre le GIP ACYMA à partir du 1er janvier prochain.

En ce qui concerne le bilan des actions des collectivités, j'insiste pour que, dans l'analyse des chiffres, vous regardiez ceux qui ont changé d'opérateur, ceux qui ont changé de technologie d'accès. Vous verrez que c'est un déclic plus facile et c'est un facteur très

important pour la réussite des politiques régionales, nationales et départementales de transformation numérique.

M. Philippe Latombe, rapporteur. La protection des données est un sujet qui m'importe beaucoup. Les collectivités territoriales collectent de nombreuses données concernant les citoyens et les usagers, notamment lorsque les communes s'occupent de crèches, de restauration collective.

Lorsque vous êtes obligés de recourir à des entreprises pour protéger les serveurs, les données, comment passez-vous vos appels d'offres ? Pouvez-vous ou non privilégier des entreprises que vous connaissez, plutôt françaises ou européennes ? Que serait-il utile de changer dans le code de la commande publique, si nous le pouvons, pour vous faciliter le travail sur ce sujet ?

En effet, nous n'avons pas encore abordé le sujet de la commande publique. Étant au plus près des territoires, vous êtes de ceux qui peuvent le plus favoriser l'émergence de solutions territoriales. La commande publique étant un bon levier, je voudrais savoir ce que vous en pensez et si vous avez des suggestions. Proposer des solutions opérationnelles est aussi la raison d'être de cette mission.

Mme Valérie Nouvel, vice-présidente du département de la Manche, représentante de l'ADF. En matière de commande, comme nous l'avons déjà dit dans d'autres instances, il faut sortir de la démarche des appels à projets parce qu'elle ne permet pas d'avoir une commande de qualité et n'assure pas la pérennité nécessaire au déploiement de ces solutions numériques. Nous sommes partisans d'intégrer, notamment dans les contrats État-région, des volets numériques beaucoup plus forts pour donner une visibilité sur le financement de projets.

Ce premier échelon est important car, en partant sur cette logique d'appel à manifestation d'intérêt (AMI), les partenaires que nous mettons autour de la table pour qu'ils répondent et se positionnent ne sont pas forcément les meilleurs pour répondre à un projet, notamment pour assurer sa pérennité dans le temps.

Les pôles de compétitivité dans les régions apportent des savoir-faire, des solutions extrêmement intéressantes du point de vue du numérique et le code des marchés publics ne nous aide pas à les mobiliser. Il faudrait arriver à rendre ce processus plus facile.

Les collectivités recourent également peu au dialogue compétitif dans le cadre de la commande. C'est dommage. Les services de collectivités peinent à l'utiliser car cela leur fait courir des risques. Pour se protéger, ils préfèrent ne pas y avoir recours. Il faudrait donner confiance dans la capacité du dialogue compétitif à apporter des réponses adéquates et des réponses innovantes sur ces questions numériques.

Par exemple, pour les solutions de coffre-fort au niveau de l'usager plutôt que dans de gros centres de données éloignés, il faut que nous puissions passer une commande de ce type. C'est compliqué dans les formes classiques de l'appel d'offres alors que, en donnant un objectif de performances qui peut justement être un objectif de sécurité du dispositif, nous pourrons à travers le dialogue compétitif voir émerger des solutions innovantes s'appuyant sur des acteurs économiques locaux. Cette mobilisation du savoir-faire français a été réalisée sur le projet NexSIS, ce qui a permis de bâtir un système souverain français intéressant.

M. Ariel Turpin, délégué général de l'AVICCA. Il est très difficile de faire des choix avec le code actuel des marchés publics. Nous en venons parfois à envier l'État qui peut

imposer aux opérateurs de ne pas choisir tel ou tel équipementier même si c'est laborieux et peut-être finalement coûteux. Nous sommes une association d'élus. Nous ne sommes pas complètement soumis au code des marchés publics mais nous devons tout de même faire de la mise en concurrence à partir d'un certain montant.

Lors du confinement, nous avons dû chercher pour une plateforme où étaient stockées les données. Cela a été très compliqué. L'information la plus claire et la plus fiable a été obtenue avec l'outil GoToMeeting, avec un hébergement en Angleterre qui reste donc européen.

Les acteurs n'ouvrent pas facilement les solutions. Peut-être pourrait-il exister des solutions labellisées par l'ANSSI ? Je ne vois pas vraiment de solution puisque, de toute façon, le code des marchés publics imposera toujours de choisir la meilleure offre.

M. Philippe Latombe, rapporteur. Sans nous heurter au droit européen, que pouvons-nous modifier dans le code des marchés publics pour vous aider ?

Mme Valérie Nouvel, vice-présidente du département de la Manche, représentante de l'ADF. Il faut peut-être plutôt travailler sur le dialogue compétitif, sur une circulaire qui donne des clés de bonne utilisation de cette forme de marché public pour des applications numériques. Peut-être pourrions-nous créer un groupe de travail sur ce sujet. Il s'agirait de définir comment formuler des attentes en matière de numérique *via* le dialogue compétitif. Nous ne sommes pas forcément obligés de modifier le code des marchés. Nous pourrions expliquer comment mieux l'utiliser dans le contexte du numérique.

Dans d'autres domaines, nous avons déjà eu des circulaires pour expliquer comment utiliser le code des marchés pour répondre à certains objectifs de déploiement de service public des collectivités. C'est un chantier intéressant à mener puisque, si Ariel Turpin se pose ces questions, c'est effectivement qu'il faut sortir un guide pragmatique que l'AVICCA pourrait diffuser auprès des collectivités.

M. Ariel Turpin, délégué général de l'AVICCA. Il faudra tout de même ajuster certaines dispositions. Ainsi, la règle selon laquelle, pour pouvoir être acceptée, l'entreprise devait présenter telle ou telle référence a déjà été attaquée et est interdite maintenant par la jurisprudence. Vous ne pouvez donc par exemple pas demander à un prestataire d'avoir prouvé sa capacité de résistance à des attaques. C'est impossible parce que c'est une barrière à l'entrée pour un nouvel entrant.

Dans tout ce que nous avons essayé de faire autour de la fibre, quelqu'un vient toujours attaquer et dénoncer le marché attribué ce qui conduit à une jurisprudence interdisant ce que nous essayons de faire.

M. Mickaël Vaillant, conseiller en charge des questions numériques de Régions de France. La question du code des marchés publics pose la question des conditionnalités ou des critères que nous pouvons introduire dans nos marchés.

Le premier point est le risque de contradiction avec la réglementation européenne. Dans cette hiérarchie de normes, il est important que cette réflexion sur l'intégration des enjeux de sécurité numérique dans la réglementation parte d'une démarche européenne, communautaire pour que nous puissions transposer sereinement dans la législation française d'éventuelles conditions particulières.

La discussion sur les conditionnalités et les critères connaît un regain avec notamment la conditionnalité des aides économiques liées aux enjeux de transition énergétique, de transition environnementale, de décarbonation. Il se trouve que le Sénat a également cet après-midi une audition sur ce sujet.

Nous réfléchissons avec les directions juridiques des régions. Deux approches sont possibles. La première est la norme obligatoire, contraignante ; il faudrait confier une mission à la direction générale des collectivités locales (DGCL) avec l'appui de l'ANSSI et de l'ARCEP pour savoir comment faire évoluer les normes. La deuxième est l'approche par les bonnes pratiques. Au-delà des critères qui tombent assez facilement sous le coup de la loi et ne sont pas compatibles avec le code des marchés publics tel qu'il existe actuellement, nous utilisons beaucoup dans les conseils régionaux les bonnes pratiques avec des outils de notation interne. Il n'est pas interdit, dans l'appréciation d'une offre, de s'intéresser à la question de la sécurité, de la gestion de la donnée, de la localisation des entreprises, même si cette notation interne peut être sujette à soupçons.

Une expertise à conduire avec la DGCL, la direction générale des finances publiques (DGFIP) et l'ANSSI semblerait vraiment utile compte tenu de l'ampleur et de la gravité du sujet, pour protéger l'ensemble des acteurs publics et assurer la nécessaire transparence à ceux qui candidatent aux marchés publics.

M. Philippe Latombe, rapporteur. Je vous remercie, cela répond en partie à ma question. La question du code des marchés publics et de l'accès à la commande publique est posée assez régulièrement, notamment par les TPE et PME spécialisées dans le domaine de la cybersécurité.

Souhaitez-vous aborder un autre sujet ?

M. Ariel Turpin, délégué général de l'AVICCA. Le questionnaire que vous nous avez transmis comportait une question sur les principaux risques de sécurité et la façon de les prévenir.

Le risque principal est actuellement le mode « sous-traitance opérateur commercial » (STOC). Le ministre lui-même s'en est ému car il ne peut pas faire un déplacement sans entendre parler des armoires défoncées, des boitiers ouverts, des câbles qui traînent sur la chaussée. Nous sommes en train, comme l'a dit le ministre, de gâcher ce que nous avons mis tant de temps à construire, ce pour quoi nous avons dépensé tant d'argent public. C'est lié à ce mode STOC et la principale menace aujourd'hui pour la sécurité vient donc des opérateurs eux-mêmes, par la sous-traitance à des sous-traitants de sous-traitants, donc finalement à des gens payés au lance-pierre, pas formés, qui doivent faire énormément de raccordements à la fibre dans la journée et massacrent complètement les réseaux. Il existe même maintenant sur internet des tutoriels qui expliquent comment aller soi-même dans l'armoire réparer sa connexion coupée lors du raccordement d'un voisin. Du coup, en réparant, vous coupez la connexion du voisin et ainsi de suite. C'est la menace la plus importante pour nos réseaux, avant la cybersécurité.

M. Philippe Latombe, rapporteur. Je vous remercie de votre présence. Nous essaierons d'être concrets et de répondre au mieux à vos interrogations et à vos besoins.

Audition, ouverte à la presse, de M. Sébastien Soriano, président de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), et de M. Jean Cattan, conseiller *(10 décembre 2020)*

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Mes chers collègues, nous auditionnons M. Sébastien Soriano, président de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP). Il est accompagné de l'un de ses conseillers, M. Jean Cattan. Cette audition s'inscrit dans le cadre des réflexions que nous menons sur la souveraineté numérique, notion qui recouvre les enjeux relatifs à la régulation des infrastructures et des plateformes numériques.

Monsieur le président, nous sommes très heureux d'échanger avec vous sur ces questions. Nous souhaitons que vous partagiez votre expérience à la tête de cette autorité administrative indépendante.

M. Philippe Latombe, rapporteur. Merci de votre présence parmi nous, monsieur Soriano. Je me réjouis moi aussi que nous ayons la possibilité d'échanger avec l'ARCEP.

Je souhaite évoquer, à titre liminaire, plusieurs enjeux sur lesquels nous aimerions vous entendre.

D'abord, quel sens revêt pour vous la notion de souveraineté numérique ? Ce concept, que l'on rapproche parfois de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique, sans devoir se soumettre aux contraintes imposées par certains acteurs publics – y compris des États – ou privés, tels que Google, Apple, Facebook, Amazon et Microsoft (GAFAM). Que pensez-vous de la montée en puissance de cette thématique dans le débat public ? Quelles seraient, selon vous, les questions prioritaires à aborder dans ce domaine ?

Ensuite, j'aimerais revenir avec vous sur le déploiement des réseaux fixes et mobiles : la souveraineté numérique recoupe directement la question de l'accès aux réseaux de communications électroniques. Notre objectif est de nous assurer que chacun dispose d'un accès de qualité et qu'aucun risque systémique ne vienne entraver le bon fonctionnement des réseaux. Nous aimerions donc que vous dressiez un état des lieux du déploiement, en lien avec le plan France très haut débit, le « New Deal mobile » et la 5G, mais aussi que vous évoquiez les différents risques de sécurité susceptibles d'affecter nos infrastructures, et les moyens prospectifs propres à nous en prémunir.

Enfin, il me semble important d'évoquer avec vous la dimension européenne et internationale de la souveraineté numérique, comme le rappelle l'intitulé même de notre mission d'information. Dans cette perspective, j'aimerais connaître votre avis sur les projets européens de régulation des acteurs du numérique. Je pense en particulier au *Digital Services Act* (DSA), qui a été présenté par la Commission européenne, et aux discussions qui se poursuivent concernant la fiscalité du numérique, notamment dans le cadre de l'Organisation de coopération et de développement économiques (OCDE). Il nous semble utile, de même, de faire un point ensemble sur les enjeux du quinzième Forum sur la gouvernance de l'internet, qui avait pour thème cette année « Un internet pour la résilience et la solidarité humaines ».

M. Sébastien Soriano, président de l'ARCEP. C'est un plaisir de répondre à vos questions.

Qu'est-ce que la souveraineté numérique ? Je vais essayer de vous proposer une réponse personnelle, car c'est un exercice d'interprétation.

Je ne voudrais pas vous effrayer avec des références gauchistes, mais il se trouve que, l'été dernier, j'ai lu le cours au Collège de France de Pierre Bourdieu consacré à l'État. Le rôle d'un État, écrit-il, est d'être la banque centrale du capital symbolique accumulé par une nation. Cette définition me semble très parlante : l'État, c'est l'endroit où une communauté humaine centralise le symbolique, c'est-à-dire un ensemble des normes et de lois, mais également de choix dans divers domaines. Cela implique également des nominations et un certain nombre de processus démocratiques.

La souveraineté, selon moi, renvoie à cet ensemble de conditions qui permettent à l'État de jouer son rôle de banque centrale du capital symbolique. Excusez-moi de faire un peu de théorie, mais votre question était fondamentale ; cela m'amène assez loin.

M. Philippe Latombe, rapporteur. C'était un peu l'objectif !

M. Sébastien Soriano. Le tout est donc de savoir si, dans le numérique, ces conditions sont remplies, et si tel n'est pas le cas, lesquelles font défaut.

Dans nos sociétés démocratiques modernes, la première souveraineté à laquelle il faut être attentif, c'est celle des individus, en particulier leur capacité à faire des choix. Le citoyen, dans nos institutions, doit pouvoir jouer son rôle, exercer son libre arbitre, dans la sphère réelle comme dans la sphère virtuelle. Or, dans le numérique, cette souveraineté des individus est, selon moi, gravement entravée par le fait que l'on est passé d'un espace public et ouvert à un espace privatisé et cloisonné.

Parfois, j'entends dire qu'il faudrait réguler le « Far West du numérique ». Mais le numérique, c'est justement tout, sauf un Far West : la plupart des problèmes tiennent au fait que l'espace virtuel a été mis en coupe réglée par quelques grands acteurs. Sous leur impulsion, le réseau, qui était extrêmement décentralisé, a connu une recentralisation : alors que, dans les premiers temps d'internet, le pouvoir avait été donné aux individus – c'est à cette époque-là, à la limite, que l'on aurait pu parler de Far West –, les grands acteurs d'internet ont installé de véritables gares de triage. Certes, ils ont permis à chacun de se repérer dans cet espace, ce qui est très important, et de mettre en relation différents acteurs grâce aux plateformes, mais, ce faisant, ils ont pris le pouvoir et recentralisé.

Mon premier souci est là : comment redonner le pouvoir aux individus, notamment par la régulation ? Dans le domaine économique, la logique même de la concurrence conduit à éviter la constitution de monopoles, pour que le seul arbitre soit, in fine, le consommateur. Or, dans le numérique – et même si l'enjeu dépasse l'aspect économique –, force est de constater que le consommateur n'a pas vraiment la possibilité de choisir entre divers acteurs.

Par ailleurs, un certain nombre d'instruments permettant l'expression de la souveraineté sont potentiellement remis en cause par le numérique – cela renvoie notamment à des enjeux de cybersécurité, question qui ne relève pas directement de ma compétence.

Je trouve intéressantes les prises de position récentes du Quai d'Orsay en la matière. Ainsi, l'ambassadeur chargé du numérique a publié un texte dans lequel il pose les bases d'une diplomatie française s'appuyant sur les communs numériques. Il s'agit de renouer avec l'idée

d'un numérique dans lequel il n'y aurait pas de contrôle, ni de la part des Big Tech ni de la part des États, d'essayer de se neutraliser mutuellement et de recréer un espace partagé. Le fait que l'on puisse concevoir cela comme un objectif diplomatique m'a beaucoup interpellé. C'est très intéressant, particulièrement à un moment où deux grands modèles s'affrontent : d'une part, le modèle des États-Unis, qui consiste, comme je l'indiquais, à privatiser l'espace numérique ; d'autre part, le modèle de la Chine qui est bâti à partir de l'État, potentiellement synonyme de censure et de surveillance. Le fait que la France et l'Europe – car nous ne réussirons pas seuls – travaillent, au niveau diplomatique, à faire en sorte que le numérique redevienne un espace partagé et ouvert, me semble essentiel pour garantir la souveraineté numérique.

En ce qui concerne le déploiement des réseaux, les progrès sont tout à fait notables. Quand j'ai pris la tête de l'ARCEP, il y a six ans, la France était dernière au classement européen du très haut débit et avant-dernière pour la 4G. Depuis lors, la relance de l'investissement a été extrêmement puissante. L'ARCEP n'a pas ménagé sa peine pour le stimuler, à travers un jeu d'incitations, parfois aussi de contraintes pour les opérateurs. L'investissement dans le secteur des télécoms est passé de 7 milliards d'euros en 2014 à 10,5 milliards d'euros en 2019, soit une augmentation de 50 %.

S'agissant de la fibre optique, environ 16 millions de prises ont été installées au cours des cinq dernières années. Selon les chiffres publiés récemment par l'IDATE DigiWorld, la France est, en valeur absolue, le pays d'Europe où la fibre se déploie le plus. Des pays comme l'Allemagne, le Royaume-Uni ou l'Italie sont quasiment au niveau zéro ; l'Espagne est plus avancée. Parmi les grandes nations européennes, la France fait figure de leader dans le déploiement des réseaux. Cela montre qu'une belle dynamique a été enclenchée.

De la même manière, notre pays a connu un accroissement très fort de la couverture 4G par les quatre opérateurs qui en sont chargés. En surface – nous avons cessé de mesurer la couverture en pourcentage de la population, car les élus locaux nous disaient que cela ne voulait rien dire, et ils avaient raison –, nous sommes passés de 46 % en 2018, au moment de la signature du « New Deal mobile », à 76 % au milieu de l'année 2020. La progression est donc spectaculaire : notre pays était classé vingt-sixième sur vingt-huit, il se situe maintenant en milieu de tableau.

La 5G donne lieu à un débat intense quant à l'intérêt de cette technologie. Le déploiement est désormais engagé. Nous avons invité les opérateurs à travailler en bonne intelligence avec les maires, y compris ceux qui s'opposaient au déploiement, pour avancer dans la concertation, ce qu'ils ont fait. Les difficultés sont en train de se dénouer : en dépit des réticences initiales, notre pays me semble bien engagé dans la 5G. Il n'en faudra pas moins rester à l'écoute des inquiétudes de nos concitoyens. La 5G sera déployée dans les zones denses et dans les zones périurbaines ou rurales accueillant des industries : tel est le schéma que nous avons construit dans les cahiers des charges. En parallèle, le réseau 4G connaîtra un double mouvement dans les zones rurales : d'abord, il continuera à s'étendre grâce au « New Deal mobile » : des milliers de sites seront construits ; ensuite, il montera en capacité avec l'arrivée de la 4G +, qui quadruplera le débit réglementaire. Pour dire les choses simplement, la 5G des villes et la 4G + des champs offriront un service quasiment équivalent dans toute la France. Nous avons ainsi veillé à éviter l'apparition de fractures territoriales.

Quels sont les risques pesant à moyen terme sur ces infrastructures ?

Le réseau mobile a été la cible d'un certain nombre d'attaques, souvent par amalgame avec la 5G. Un réseau de télédiffusion a même été attaqué pour cette raison, alors qu'il n'avait évidemment rien à voir avec cette technologie. Il faut donc être vigilant sur ce point, mais je

ne suis pas en mesure de formuler devant vous des préconisations précises à ce propos, monsieur le rapporteur. Sans doute les opérateurs devront-ils sécuriser davantage leurs sites.

S'agissant des réseaux de fibre optique, le risque tient au fait qu'ils ont été construits par une pluralité d'acteurs, contrairement à ce qui s'est passé pour le réseau téléphonique qui s'est développé dans le cadre d'un monopole. Nous soutenons ce modèle pluraliste, car il a produit une saine émulation, permettant de combiner les énergies pour couvrir autant de territoire que possible. Toutefois, il soulève deux questions.

Premièrement, les règles d'ingénierie utilisées pour la construction des premiers réseaux de fibre mériteraient peut-être d'être revues. À cet égard, le secrétaire d'État Cédric O a confié à Benoît Loutrel une mission portant notamment sur les réseaux d'initiative publique. Cela permettra de faire remonter des problèmes éventuels.

Deuxièmement, à moyen terme, on peut s'interroger sur les capacités d'intervention en cas d'accident. Quand des inondations détruisent une route, emportant avec elle l'ensemble des infrastructures, France Télécom est en mesure de mobiliser ses équipes, y compris en les faisant venir d'autres territoires. Pour réparer un réseau purement local, on ne peut compter que sur les équipes d'intervention attachées à sa maintenance. La solidarité entre les réseaux est donc un enjeu essentiel : il faut créer des mécanismes d'intervention permettant de faire face aux crises. Nous interpellons régulièrement le Gouvernement, sans avoir obtenu, jusqu'à présent, un réel suivi de ce problème.

J'en viens à la dimension européenne, qui est évidemment essentielle dès lors que l'on évoque les enjeux numériques. Que penser des projets européens de DSA (*Digital Services Act*) et de DMA (*Digital Markets Act*) ? Il importe, au préalable, de bien distinguer les deux.

Pour ce qui est du DSA, la direction choisie est la bonne. Elle consiste, pour la gestion des contenus – notamment sur les réseaux sociaux –, à construire quelque chose à côté des procédures judiciaires. Celles-ci visent à traiter les contenus illicites ; cela doit continuer. Le Gouvernement a d'ailleurs annoncé une augmentation des moyens affectés à cet effet, avec le recrutement de magistrats supplémentaires et le renforcement des équipes de la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS), chargée des interventions administratives sur les contenus. Mais on voit bien que ce n'est pas suffisant : il reste beaucoup de contenus « gris », qu'il n'est pas facile de juger, notamment quand il s'agit de caractériser le discours de haine.

Par ailleurs, l'enjeu n'est pas seulement d'interdire certains contenus : il faut aussi, potentiellement, limiter leur viralité. Pour cela, il ne suffit pas d'édicter un règlement ; on doit également s'appuyer sur l'intelligence des plateformes. Celles-ci doivent être des régulateurs de premier niveau, au-dessus desquels il y aurait un régulateur de second niveau, à savoir une autorité publique s'assurant que le travail a été bien fait au premier niveau. On appelle parfois cela « régulation-supervision ». C'est un peu ce qui existe dans le domaine bancaire : les acteurs ont leur propre modèle de gestion du risque, contrôlé par l'Autorité de contrôle prudentiel et de résolution. Telle est la voie choisie par le DSA. L'ARCEP soutient depuis longtemps cette démarche.

Un point, toutefois, mérite notre vigilance. Un débat va avoir lieu à l'échelon européen pour savoir quels types de contenus doivent faire l'objet de cette supervision. Or il peut y avoir, à cet égard, des différences de culture entre le nord et le sud de l'Europe. Si on se limite aux contenus illicites, le dispositif ne servira à rien : la réponse doit d'abord être judiciaire. Il faut donc élargir le cercle des contenus visés. Il conviendra d'être vigilant sur ce point lors des négociations.

Le deuxième volet, le DMA, vise à renforcer la régulation économique et la concurrence. Je dois partager avec vous ma grande inquiétude sur ce texte : en l'état, il n'apporterait qu'un progrès limité en faisant de la réglementation plutôt que de la régulation. Il viserait à imposer aux grandes plateformes certaines règles pour les empêcher d'écraser les petites et moyennes entreprises (PME) qui travaillent avec elles. Il s'agirait par exemple d'éviter que Google, dans sa plateforme publicitaire Adwords, change les règles de gestion des contenus et des délais de préavis pour le déréférencement de certains acteurs, ou encore d'obliger Amazon à faire preuve de loyauté dans sa relation avec les PME. Tout cela est nécessaire, mais c'est totalement insuffisant pour changer le paysage numérique : on limite la casse en encadrant les interactions des monopoles avec le reste de l'économie, mais on ne règle pas le problème de fond, à savoir l'existence de monopoles.

Pour ce faire, il faut créer des instruments proactifs, comme on l'a fait dans les télécoms il y a vingt-cinq ans. Il faudrait se doter d'un régulateur, d'une agence européenne qui serait chargée de casser les monopoles en établissant des règles de séparation et d'interopérabilité, afin de passer d'un système centralisé à une véritable concurrence entre différentes entités. Le DMA n'en prend pas le chemin, d'où mon inquiétude.

Pour ce qui est des discussions sur la fiscalité du numérique dans le cadre de l'OCDE, ce n'est pas un sujet que je suis de près. La clef se situe aux États-Unis. On peut espérer qu'avec l'arrivée de Joe Biden, les négociations progressent et permettent enfin d'envisager l'adoption d'une fiscalité assise sur la réalité économique locale de l'activité et de ses acteurs.

Le Forum sur la gouvernance d'internet est une enceinte extrêmement utile en ce qu'elle permet de débattre et de conserver un lien avec la société civile, sans laquelle rien n'est possible dès lors qu'internet est en jeu. Pour notre part, nous y sommes très actifs lorsqu'elle se réunit. Nous avons participé cette année à l'émergence d'une prise de conscience sur les enjeux environnementaux du numérique et sur la manière d'accompagner le secteur numérique vers davantage de sobriété.

M. Philippe Latombe, rapporteur. Vous avez laissé entendre que les pays du nord et du sud pouvaient avoir des positions différentes sur le contenu du *Digital Services Act* et sur la possibilité de l'étendre à d'autres domaines. Le Gouvernement français voudrait transposer quasiment immédiatement le projet de directive, avant même que le trilogue ait donné lieu à un accord. Quelles précautions devrait prendre le législateur pour éviter une éventuelle surtransposition par rapport au texte qui sera finalement adopté au niveau européen ? Doit-on montrer l'exemple en le transposant de façon large, même si une négociation doit intervenir par la suite ? Quelle est la position de l'ARCEP sur cette question ?

M. Sébastien Soriano. Je vous ferai une réponse toute personnelle : si la France veut agir ainsi, elle doit faire amende honorable sur ses errements passés, notamment lors du vote de la proposition de loi « Avia ». Le Gouvernement a envoyé des signaux assez négatifs aux acteurs qui sont sensibles aux enjeux de liberté numérique – sans même parler pas de la proposition de loi relative à la sécurité globale, qui soulève encore d'importantes inquiétudes en la matière.

La proposition de loi « Avia » a été extrêmement mal préparée, puisque l'idée d'une régulation-supervision était déjà sur la table. Mme Avia a tenu absolument à garder la disposition relative au retrait des contenus en vingt-quatre heures, qui était un mélange des genres entre le judiciaire et la régulation. C'est la raison pour laquelle le Conseil constitutionnel l'a censurée : en confiant un rôle de censeur aux plateformes, elle les conduirait immanquablement à surcensurer pour ne pas s'exposer à des sanctions. Il est très important que la France fasse comprendre, en interne comme à l'extérieur, qu'elle a compris comment

il fallait gérer ce sujet et qu'elle ne cherche pas à répéter l'erreur de la loi « Avia ». Alors seulement, elle pourra montrer l'exemple. Si, en revanche, elle se contente de ressortir la loi Avia et de lui mettre un coup de peinture, alors elle n'enverra pas le bon signal.

Mme Laure de La Raudière. J'étais dans l'hémicycle, avec M. le rapporteur, lors de l'examen de la proposition de loi « Avia » : autant nous avions trouvé que l'article 2, qui donnait de nouveaux pouvoirs au CSA (Conseil supérieur de l'audiovisuel), était réellement intéressant, autant le cœur même de ce texte ne nous avait pas paru bon, pour les raisons que vous venez d'évoquer.

Je voudrais revenir sur ce qu'il sera possible de défendre au niveau français. Lors des débats sur le projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière économique et financière (DDADUE), l'article 4 *bis* a été supprimé au motif que ses dispositions seraient adoptées au niveau européen, dans le cadre du futur DMA. Pensez-vous qu'il sera tout de même possible d'adopter certaines mesures au niveau français, dans l'hypothèse où le DMA ne serait pas suffisamment ambitieux ?

M. Sébastien Soriano. Sur le plan de la compatibilité avec la directive e-commerce, il nous paraît possible d'adopter une régulation de type supervision des contenus en retenant un périmètre raisonnablement large. Dès lors que l'existence d'un motif d'ordre public peut être démontrée, par exemple en matière de haine, cela nous paraît jouable. Autrement dit, si la proposition de loi « Avia » s'était limitée à l'article 2 – autrement dit à son périmètre initial, celui de la haine en ligne, avant que des amendements ne viennent y rajouter toute une série d'autres sujets –, elle aurait été compatible avec la directive e-commerce.

De la même manière, les dispositions sur les terminaux et l'interopérabilité contenues dans la proposition de loi « Primas » sont tout à fait compatibles avec la directive e-commerce. D'ailleurs, le Gouvernement s'est opposé à ce texte non pas en raison d'une éventuelle incompatibilité, mais surtout pour une raison d'opportunité, afin d'éviter de transposer par anticipation.

En revanche, une fois qu'une proposition de texte de la Commission européenne est sur la table, les conditions de compatibilité sont durcies. Chaque État membre ayant un devoir de coopération, il n'est pas censé agir en anticipation. Cela mériterait sans doute une analyse juridique plus fine mais, à partir du 15 décembre, le terrain sera sans doute un peu plus glissant pour la France si elle se retrouve à devoir transposer de façon anticipée le DSA ou le DMA.

Mme Laure de La Raudière. Cela vaut pour la neutralité des terminaux. Mais, s'agissant de l'interopérabilité, peut-on agir tout en restant dans le cadre de la directive e-commerce ? L'interopérabilité est un enjeu de souveraineté et de mobilité déterminant. Comment peut-on l'imposer de façon plus efficace et plus systémique aux plateformes, sachant que de nouvelles techniques rendent cette opération plus facile ?

M. Sébastien Soriano. Nous ne voyons pas d'incompatibilité de principe avec la directive e-commerce.

Mme Danièle Hérin. Vous avez dit l'essentiel, en particulier sur le rôle que pourra jouer la France. Cela permet de se positionner en connaissance de cause.

M. Philippe Latombe, rapporteur. J'aurais une dernière question sans doute connexe – il faudra étudier avec le président la possibilité d'ouvrir un nouveau chapitre sur ce sujet – à propos des nouveaux moyens de communication que représentent les constellations de satellites. Les Américains sont très en avance ; ils ont un modèle un peu particulier, avec des lanceurs privés indirectement subventionnés par l'État par le biais de lancements

gouvernementaux, ce qui fait bénéficier les lancements commerciaux de tarifs ultra-compétitifs. Des entreprises privées, comme celle d'Elon Musk, lancent des constellations de satellites pour pouvoir ensuite faire du réseau internet.

L'Europe semble à la traîne, et pourtant le commissaire européen Thierry Breton veut lancer une constellation européenne. Que doit-on faire pour accompagner cette volonté ? Comment garantir que sa construction se fera de façon souveraine ? L'ARCEP a-t-elle un avis ou des préconisations à faire sur ces nouveaux modes de communication ?

M. Sébastien Soriano. Pas vraiment, malheureusement, car nous n'avons qu'une compétence très restreinte en matière de satellites, puisqu'elle se limite à l'autorisation donnée aux équipements au sol de communiquer avec les satellites.

Pour ce qui est de la souveraineté française, il ne me semble pas que ces constellations présentent un réel danger dans la mesure où elles arriveront dans un calendrier trop tardif par rapport à la stratégie de couverture du territoire dans laquelle la France est engagée : autrement dit, notre pays sera quasiment intégralement fibré quand ces satellites commenceront à fournir un service pertinent. Il n'y a donc pas de risque de dépendance de notre pays vis-à-vis de ce type de technologie.

Le risque est plutôt celui d'une perte d'opportunité : ces constellations vont certainement jouer un rôle important pour la connectivité des pays en voie de développement et pour certains usages, maritimes et autres. La prédominance américaine sur le contrôle des communications pose-t-elle question dans l'équilibre géostratégique ? Cela me dépasse assez largement.

M. Philippe Latombe, rapporteur. Le rôle de l'ARCEP porte plutôt sur la partie récepteurs, sachant que très peu de récepteurs de ce type sont construits en Europe, la plupart étant d'origine américaine.

M. Sébastien Soriano. Je me réjouis que l'Assemblée nationale se saisisse de ce sujet : nous sommes à votre disposition pour tout éclaircissement ultérieur.

M. Philippe Latombe, rapporteur. Ce sera avec grand plaisir ! Je vous remercie pour le temps que vous nous avez consacré.

Audition, ouverte à la presse, de M. Didier Patry, directeur général de France Brevets, de MM. Guillaume Ménage et Vincent Puyplat, directeurs adjoints, et de Mmes Anne-Sophie Sebire, directrice juridique, et Audrey Lenne, directrice conseil au sein du cabinet Rivington
(17 décembre 2020)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Nous auditionnons aujourd'hui France Brevets, une société fondée en 2011, détenue par l'État et la Caisse des dépôts et consignations, dont la mission est « *d'accompagner les entreprises dans la valorisation de leurs innovations par la structuration de leur propriété intellectuelle et par sa défense à travers le monde* ».

Sont présents pour cette visioconférence M. Didier Patry, directeur général de France Brevets, les deux directeurs adjoints M. Guillaume Ménage et M. Vincent Puyplat, Mme Anne-Sophie Sebire, directrice juridique, et Mme Audrey Lenne, directrice conseil au sein du cabinet Rivington.

Cette audition s'inscrit dans le cadre des réflexions que nous menons sur la souveraineté numérique. Cette notion recouvre non seulement les sujets classiques relatifs à nos infrastructures, sujets que nous avons déjà largement explorés, mais aussi les enjeux propres à la protection et à la valorisation de la propriété intellectuelle, c'est-à-dire des brevets déposés par nos entreprises.

Dans ce cadre, nous nous réjouissons, monsieur le directeur général, de pouvoir échanger avec vous et votre équipe sur votre conception de la souveraineté numérique française et européenne et sur la façon dont France Brevets peut contribuer à la promouvoir. Je souhaite que ce moment d'échange nous permette également d'aborder votre actualité pour l'année 2021 et la façon dont la crise de la covid a pu impacter vos activités en 2020.

J'aimerais d'abord que vous nous présentiez France Brevets et son activité, en insistant notamment sur le dispositif de la Fabrique à brevets destiné aux start-up et aux petites et moyennes entreprises (PME) de la Tech à fort potentiel. Nous aimerions aussi savoir de quelle façon vous vous êtes organisés pour poursuivre votre activité dans le cadre de la crise épidémique, notamment comment vous anticipez les mois à venir.

Je voudrais ensuite vous interroger sur la façon dont vous concevez la souveraineté numérique française et européenne. Ce concept, parfois rapproché de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et à ne pas subir les contraintes imposées soit par des acteurs publics comme les États soit par les acteurs privés que sont les géants du web (GAFAM). Je voudrais savoir de quelle façon cet impératif croissant peut se traduire au sein de votre secteur d'activité, notamment pour les start-up.

Enfin, je souhaite aborder avec vous la question de l'innovation qui est au cœur de la souveraineté technologique de la France et de l'Europe. D'après les données du dernier tableau de bord européen de l'innovation (TBEI) qui comprend 27 indicateurs distincts, la France se classe dans le groupe des innovateurs notables avec des pays comme l'Allemagne, l'Autriche, la Belgique ou l'Estonie. Quel regard portez-vous sur nos performances nationales ? Le cas échéant, comment serait-il possible de nous rapprocher encore plus du haut du classement, c'est-à-dire des champions de l'innovation que sont le Danemark, la Finlande, les Pays-Bas et la Suède ?

J'aimerais aussi vous entendre sur les performances européennes comparées à celles de nos concurrents directs, la Chine et les États-Unis. Nos échanges sur ce point devraient nous permettre de dresser ensemble le bilan des secteurs dans lesquels les entreprises françaises et européennes déposent le plus ou le moins de brevets et d'évoquer les moyens de les encourager à innover encore davantage.

M. Didier Patry, directeur général de France Brevets. France Brevets a une assez petite équipe de 17 personnes. Nous sommes essentiellement logés à Paris, dans le 9e arrondissement, près de la gare Saint-Lazare. La société travaille avec un nombre important de consultants, avec des personnalités extérieures et avons une présence en Chine, en Corée et au Japon ainsi qu'en Amérique du Nord et au Canada. Les personnes situées dans ces pays ne sont techniquement pas des employés de France Brevets mais des consultants que nous utilisons durant 60 % à 80 % ou 90 % de leur temps.

Nous faisons de plus appel à un certain nombre de consultants dans le domaine de la technologie ou du droit, à beaucoup d'avocats et de conseils en propriété intellectuelle. Comme nous devons traiter des dossiers technologiquement complexes, nous devons d'abord être professionnels ce qui nous impose de nous référer à des personnes de référence dans leur domaine. Nous faisons donc régulièrement appel à des consultants de très haut niveau dans des domaines technologiques très spécifiques tels que le transport, l'automobile, les véhicules autonomes, les batteries ou la physique quantique ou l'informatique quantique ou la cybersécurité.

Nous avons deux actionnaires puisque France Brevets a été créée en 2011 dans le cadre du premier plan d'investissements d'avenir (PIA). Nous avions à l'époque une relation assez forte avec le Commissariat général à l'investissement (CGI) devenu maintenant le Secrétariat général pour l'investissement (SGPI). Nous avons dix administrateurs, quatre de l'État, quatre de la Caisse des dépôts et consignations et deux administrateurs du privé, dont notre président Olivier Appert.

Techniquement, France Brevets est une société privée, une société par actions simplifiée (SAS). Nous avons de ce fait la capacité d'être titulaires de brevets. Nous sommes aussi en mesure de rentrer dans des relations contractuelles qui peuvent être complexes et d'aller en justice. Nous représentons en justice certaines entreprises pour faire valoir leurs droits. Notre mission est de protéger et défendre l'industrie française. Quand besoin est, nous représentons des PME, quelquefois des entreprises de taille intermédiaire (ETI) pour faire valoir leurs droits dans certaines juridictions. Il est donc important que France Brevets soit une SAS pour avoir cette liberté d'action.

Nos activités principales tournent autour de la propriété intellectuelle, essentiellement des brevets. Notre première mission est de générer des modèles économiques qui permettent de satisfaire l'industrie et l'économie françaises.

Le premier point est d'apporter de la valeur. Dans nos missions, il s'agit d'abord d'axer sur la qualité et de se dire que la propriété intellectuelle n'est pas intéressante si elle n'a pas de valeur. Cela ne signifie pas qu'il faille nécessairement qu'elle rapporte de l'argent. Nous ne parlons pas nécessairement de revenu mais il faut que cette propriété intellectuelle apporte quelque chose à l'entreprise. Notre combat quotidien est d'expliquer aux sociétés françaises qu'accumuler des brevets et de la propriété intellectuelle sur des étagères ne sert à rien, qu'il est fondamental que cette propriété intellectuelle soit activée ou activable à tout moment.

Très concrètement, nous avons dans un premier temps généré des revenus pour des entreprises ou des laboratoires de recherche en monétisant de la propriété intellectuelle, donc en utilisant les portefeuilles de brevets disponibles pour générer des revenus.

Notre programme phare est le programme *Near Field Communication* (NFC), une technologie qui permet d'émuler les techniques de paiement et les transactions à courte distance. Certaines entreprises l'utilisent aujourd'hui pour payer dans les magasins, notamment avec le téléphone. Cette technologie est en grande partie une technologie française, créée par une très belle entreprise française qui a été leader de la carte à puce. Notre mandat est donc d'administrer un programme de licences et, si possible, de générer des revenus lorsque l'entreprise est titulaire de ces brevets. Deux entreprises sont concernées : une PME française et un grand groupe français de télécoms. Les licenciés sont actuellement des géants de la Tech, des télécoms. France Brevets est certainement la seule entité en France à avoir réussi à conclure ce type de contrats. Cela n'a parfois pas été sans douleur puisque, manifestement, tout le monde n'a pas envie de payer ces licences. Il faut parfois un peu montrer les muscles. Il nous faut donc aller en justice pour faire valoir les droits des entreprises que nous représentons en arguant de la contrefaçon, que nous transformons après accord en un accord de licence.

Nous nous sommes ensuite focalisés sur les entreprises à fort potentiel les plus vulnérables ce qui nous a amenés à développer le programme de la Fabrique à brevets (FaB). L'idée de base est d'équiper les start-up et PME de portefeuilles de brevets de qualité pour que ces brevets soient utilisables. C'est le principe que j'ai déjà évoqué : la propriété intellectuelle sur étagère, qui ne sert à rien, n'est pas activable ou activée, n'est pas utile. Cette propriété intellectuelle vient grever le budget de l'entreprise ou impacter négativement son compte d'exploitation. Il faut donc qu'elle ait une utilité et une efficacité. Ce n'est possible qu'à partir d'une certaine qualité et d'une certaine masse. Toutes les analyses que nous faisons nous démontrent que les entreprises les plus offensives, celles qui gagnent, jouent avec ces deux critères de quantité et de qualité. La France n'est malheureusement pas très bien placée pour ce qui est de la quantité.

Une quarantaine d'entreprises ont été analysées ou accompagnées dans le cadre de ce programme. Certaines sont maintenant sorties du programme. Nous étions jusqu'à présent en phase de test puisqu'il a fallu faire évoluer l'environnement contractuel. Nous aimerions étendre ce programme en 2021, avec l'ambition d'accueillir une trentaine d'entreprises.

Nous n'avons pu accueillir en 2020 que sept entreprises du fait de notre modèle économique : nous prenons à notre charge les frais de constitution d'un portefeuille de brevets. Il s'agit d'abord d'identifier les inventions à breveter, pas nécessairement brevetables mais qu'il est intelligent de breveter, ce qui va dans le sens de la recherche de qualité. Ensuite, nous travaillons avec nos partenaires conseils en propriété intellectuelle, qui sont les représentants juridiques de la start-up que nous épaulons, pour définir un axe, une direction, un objectif, un volume de brevets. Main dans la main, nous constituons le meilleur portefeuille de brevets au vu de la situation de la société à l'instant où nous l'assistons.

Cela signifie que nous essaierons de doter une entreprise au stade de l'amorçage d'au minimum cinq brevets puis, au fur et à mesure de son évolution, ce nombre augmentera pour aller jusqu'à quarante ou cinquante. Dans la plupart des domaines techniques, électronique, informatique, science des matériaux, mécanique, peut-être même la chimie mais pas la pharmacie et la biotechnologie, le principe de base est qu'il faut entre trente et cinquante brevets pour pouvoir peser sur les marchés.

Nous prenons donc à notre charge ces frais. Nous payons les factures des conseils en propriété intellectuelle pour la mission et l'objectif que nous nous sommes assignés, pendant une période variant entre douze et vingt-quatre mois. À la fin du contrat, nous demandons le remboursement des frais que nous avons avancés, additionnés d'une marge correspondant au service d'accompagnement et de chef de projet que nous fournissons. Techniquement, ce n'est donc ni un prêt ni une subvention. À ce stade, ce n'est pas non plus un investissement en capital puisque France Brevets ne prend pas de position au capital. C'est une avance remboursable.

Ce projet demande à évoluer car le taux de sinistralité des entreprises est assez élevé en ce moment. Nous courons malheureusement le risque de ne pas pouvoir amener ce programme à l'équilibre. Nous devons trouver un moyen de rémunération différent, supérieur à celui que nous avons actuellement. Nous y travaillons avec des fonds d'investissement. Le constat est qu'il serait bon que nous ayons des collaborations avec les fonds pour qu'ils identifient avec nous les sociétés ayant le plus fort potentiel afin que nous nous retrouvions de façon synchrone dans les cycles d'investissement.

L'idée de ce programme est aussi de doter les entreprises d'une propriété intellectuelle qui soit satisfaisante pour les investisseurs, de façon à ce qu'ils considèrent cette propriété intellectuelle comme suffisamment attractive et solide pour investir de façon sereine.

Le constat est net : le niveau de sophistication des investisseurs s'accroît car le ton est très anglo-saxon. Les Anglo-Saxons ont toujours cherché à investir dans des entreprises possédant des actifs immatériels de qualité. Cet état d'esprit arrive de plus en plus en France. Notre programme rencontre donc une demande des investisseurs et cela se traduit par des investissements, des réussites.

Nous espérons que ce programme FaB continuera et évoluera. Des entreprises nous interrogent et nous avons ainsi eu l'opportunité la semaine dernière de discuter avec l'Office de la propriété intellectuelle de Singapour qui s'intéresse à ce que nous faisons. Il trouve que ce modèle est intéressant et songe à le développer également. La Chine nous a aussi posé beaucoup de questions sur ce programme ; le ministère chinois de l'économie et de l'industrie s'y intéresse.

Nous avons donc beaucoup de satisfactions, des réussites et des échecs. Certaines des premières entreprises que nous avons aidées ont pu trouver des fonds, conclure des partenariats ce qui est important pour une toute petite entreprise. Pour conquérir des parts de marché, elle doit trouver des partenaires et certaines ont trouvé de très beaux partenaires. D'après leurs témoignages, cette propriété intellectuelle leur a permis d'avoir un dialogue plus équilibré. C'est le problème des petites entreprises : au-delà d'être toujours à la recherche de cash, il s'agit aussi de rééquilibrer le rapport de forces qui est par nature déséquilibré.

Nous avons aussi eu quelques échecs. Certaines entreprises n'ont pas réussi à survivre. Cela a été pour nous une difficulté. Pour rééquilibrer cette situation, nous devons aller chercher des revenus complémentaires. C'est le cycle naturel de la vie ; toutes les start-up ne réussissent pas. Par contre, plus nous les accompagnons et plus nous sommes présents tôt dans le cycle, plus nous avons de chances de travailler avec elles. Malheureusement, d'autres éléments interviennent dans la recette de la réussite d'une start-up : le management, l'appétence du marché, parfois des coïncidences. Lorsque plusieurs start-up arrivent avec le même produit sur le même marché, toutes ne survivent pas. Un certain taux de sinistres est donc normal.

M. Philippe Latombe, rapporteur. Quelles sont à votre avis les pistes d'évolution pour diversifier vos sources de revenus et permettre l'équilibre économique de ce

programme ? Envisagez-vous de rentrer au capital de ces structures, directement ou indirectement ? Envisagez-vous plutôt un partenariat avec les fonds en faisant de la facturation ? Prévoyez-vous de la prestation de services ou de la participation ou un mélange des deux ?

M. Didier Patry, directeur général de France Brevets. Nous envisageons un mélange des deux solutions. L'objectif *in fine* n'est pas du tout d'être au capital mais d'utiliser des instruments financiers tels que des bons de souscription d'actions (BSA) ou des obligations convertibles afin de profiter de la valorisation de l'entreprise et du cycle suivant d'investissement. À long terme, nous n'avons pas l'intention d'être au capital ni d'être un investisseur actif. Nous ne souhaitons ni diriger l'actif des entreprises ni avoir une quelconque influence sur l'entreprise.

Toutefois, vous avez raison, il existe des instruments financiers qui permettent de participer à l'évolution de la valeur de l'entreprise et d'en capter une partie sans que ce soit pénible ou difficile pour l'entreprise. De nombreuses entreprises sont prêtes à ce type de schéma, à condition que nous ne venions pas charger inutilement la partie administrative. Nous devons donc travailler avec les fonds, être synchrones avec les levées de fonds au moment où la charge administrative est la plus lourde. Nous envisageons de plus d'avoir un mécanisme de prestation de services.

Nous souhaitons que ce programme soit un véhicule d'investissement pour guider de l'argent de grandes entreprises vers de plus petites entreprises. Notre objectif est également que le tissu industriel français de moyennes et de grandes entreprises trouve sur son sol des start-up qui lui plaisent, qui l'intéressent, qui soient sujettes à des acquisitions. C'est ainsi que la mécanique économique sera dynamique et viable.

Toutes les grandes entreprises se transforment. Par exemple, les grandes entreprises électriques ont besoin d'aller vers la domotique – capter des données, véhiculer de l'information, avoir des capteurs partout – et cette croissance se fait souvent par une croissance inorganique, c'est-à-dire par l'acquisition de start-up. Il serait plus intéressant que ces grands groupes français acquièrent des start-up françaises plutôt que des start-up américaines, israéliennes, allemandes, anglaises ou chinoises par exemple. Même si c'est possible, l'acculturation et l'intégration sont toujours nettement plus difficiles.

Une telle acquisition peut faire partie d'une stratégie économique nationale et d'un jeu géopolitique mais nous ne pourrons permettre l'évolution, la croissance, la stabilité et le virage de grandes entreprises françaises que si elles trouvent sur leur sol un vivier de start-up suffisamment viables. Le programme de la Fabrique à brevets pourrait être un moyen de véhiculer de l'argent vers ces start-up et d'avoir une position de petit investisseur discret pour favoriser l'essor d'un secteur. Nous avons déjà des discussions avec des groupes qui s'intéressent à ce programme.

Il est important de noter que la start-up, dans le modèle actuel, est propriétaire de ses brevets, en reste propriétaire et en fait ce qu'elle veut. Nous n'avons pas ou très peu de leviers d'action sur ces brevets. Nous ne cherchons pas à faire de la valorisation. Nous voulons simplement que les start-up soient équipées comme il faut, avec la quantité et la qualité nécessaires donc un calibrage parfait, le plus précis qu'il est possible pour qu'elles atteignent l'objectif économique qu'elles se sont fixé.

M. Philippe Latombe, rapporteur. Pensez-vous que les PME et les grandes entreprises françaises ont suffisamment cette culture d'achat de l'immatériel comme peuvent l'avoir notamment les Anglo-Saxons ? Vous avez dit que cette culture de la qualité de

l'immatériel arrive en France. Sommes-nous en retard sur ce sujet ? Existe-t-il encore des freins ? Le fait que votre travail consiste à le promouvoir signifie qu'il a existé des freins. Sont-ils en train d'être levés, sont-ils déjà levés ?

M. Didier Patry, directeur général de France Brevets. Cette remarque est extrêmement pertinente. Effectivement, le constat est net qu'un certain nombre d'entreprises qui ont eu un très fort succès sur le marché – par exemple dans le domaine des moteurs de recherche ou du positionnement précis par GPS ou de la fourniture de taxis ou des places de marché numériques – ont eu des stratégies de brevets hybrides. Elles ont engagé des phases d'achat de brevets. Leur propriété intellectuelle s'est construite par des acquisitions, en particulier de très grosses acquisitions ayant pour but de renforcer la position de la société.

Malheureusement, force est de constater que nous sommes assez en retard. La philosophie en ce moment, dans ce pays, est plutôt une stratégie des années 1980 ou même 1970 consistant à constituer sa propriété intellectuelle à l'aide de sa recherche et développement (R&D) interne. Ce n'est pas du tout ce que font certaines entreprises du côté ouest de l'Atlantique et celles qui ont eu beaucoup de succès dans le domaine de la Tech n'ont pas procédé ainsi.

Nous devons nous imprégner de cette façon d'agir. Dans le cadre de la Fabrique à brevets, nous suggérons aux entreprises avec lesquelles nous travaillons de regarder ce sujet. Évidemment, tout n'est pas à acheter. De nombreux brevets sont sur le marché et de nombreuses ventes ont lieu actuellement. De très grandes sociétés de télécommunications, dont une société canadienne qui fut vraiment précurseur dans le domaine des télécoms, mettent leur portefeuille de brevets en vente. Un très gros opérateur allemand du domaine des télécoms et une grosse société informatique japonaise ont également mis leur portefeuille de brevets en vente. Un grand nombre de brevets sont donc sur le marché.

Il existe également des brevets à acheter dans le stock de la recherche publique française. Il faut reconnaître la qualité de nos laboratoires de recherche, en particulier d'un laboratoire dont le siège est dans le 16e arrondissement à Paris. Il est souvent remarqué même par les organismes outre-Atlantique qui notent la recherche. De brevets de qualité sont issus de la recherche française et nous pourrions imaginer que les start-up ou les PME françaises s'équipent en brevets achetés auprès de la recherche française.

Je pense important d'étudier cet axe car le retour sur investissement est intéressant. En effet, il est plus facile d'acheter quelque chose de qualité en le voyant, en pouvant le jauger, l'examiner, l'analyser. Lorsqu'une entreprise dépose une demande de brevets de sa propre R&D, elle n'a aucune idée de ce que cela donnera. Il faut attendre trois, quatre ou cinq ans pour arriver à maturité, pour que les brevets soient délivrés et pour commencer à avoir une idée de la pertinence et de l'impact des brevets. À mon avis, il faut donc acheter sur étagère. Le seul blocage est que les entreprises n'y pensent pas, surtout pour des entreprises dont un pilier important dans leur stratégie intellectuelle est de ne pas se faire copier en protégeant leurs inventions.

Toutefois, un autre pilier important est de ne pas se faire agresser. Notre stratégie est de protéger et défendre. Pour défendre, il faut avoir des moyens de défense et, souvent, ses propres brevets ne sont pas les meilleurs moyens de défense pour une entreprise agressée sur un marché lors d'une tentative de déstabilisation ou de prédation organisée par une entité quelle qu'elle soit pour racheter l'entreprise. Nous avons déjà observé ce phénomène et nous souhaitons d'ailleurs mettre sur pied un système permettant de l'éviter.

Le premier objectif à notre avis n'est plus d'éviter de se faire copier mais de ne pas se faire agresser. En effet, une agression provoque des pertes économiques importantes et, même sans décision de justice, pendant les premières années de contentieux en première instance par exemple, les coûts sont énormes. Pour vous donner un ordre d'idée, en France aujourd'hui, les frais de défense en première instance sont de 100 000 à 200 000 euros. En Allemagne, il faut compter entre 2 et 3 millions d'euros et il s'agit d'argent qu'il faut sortir tout de suite. En Chine, cela coûte entre 500 000 et 2 millions d'euros. Aux États-Unis, le coût monte entre 4 et 6 millions par an. Ce coût est une pression énorme pour une ETI, encore plus pour une PME et, pour une start-up, c'est la mort.

Pour être capable de réagir, il faut des brevets capables d'impacter l'agresseur. Les brevets issus de sa propre R&D sont rarement percutants face aux plus grands agresseurs. Cela implique de développer le pilier « Défense » en pensant à des acquisitions. Ces acquisitions de brevets ne sont pas destinées à être en relation avec sa propre activité mais avec l'activité de l'agresseur pour être capable de l'impacter, d'avoir une adhérence sur sa surface d'activité et de préférence sur sa surface d'activité la plus chère, celle qui est la plus importante pour lui. Cela permet de rééquilibrer le rapport de force.

M. Philippe Latombe, rapporteur. Aujourd'hui, votre activité va donc au-delà du conseil stratégique et s'intéresse aussi à la protection juridique, au conseil juridique préalable.

M. Didier Patry, directeur général de France Brevets. Attention, nous collaborons étroitement avec des avocats et des conseils en propriété intellectuelle mais nous ne pouvons pas aller dans un domaine d'activité qui est réglementé car nous ne sommes pas accrédités, bien que certains d'entre nous aient cette formation et cette qualification. Nous n'agissons ni en tant que conseil en propriété intellectuelle ni en tant qu'avocat. Nous nous refusons à donner des avis de droit et nous ne le ferons pas.

Par contre, il existe une ingénierie du droit, une gestion des activités très liées au juridique par association avec un conseil en propriété intellectuelle ou un avocat. Nous constatons que, malheureusement, surtout vis-à-vis des avocats, la perception dans ce pays est trop souvent que les avocats servent à faire sauter des amendes ou à régler des problèmes de divorce.

L'avocat, comme le conseil en propriété intellectuelle, est un stratège. Tous deux ont une vision stratégique et sont indispensables pour formuler une stratégie non pas d'entreprise mais d'ingénierie juridique, que ce soit pour se protéger ou pour être à l'offensive. Nous incitons donc très fortement les entreprises à travailler avec un avocat et/ou un conseil en propriété intellectuelle en fonction des besoins, selon s'il s'agit de déposer un brevet, une marque, un modèle ou d'un besoin plutôt d'architecture contractuelle ou de préparer un contentieux ou une offensive.

L'important pour nous est surtout que la direction de l'entreprise s'approprie la stratégie juridique. C'est rarement le cas. Soit il existe un ou une juriste dans l'entreprise qui est capable d'architecturer cette ingénierie, soit il n'en existe pas et c'est souvent le cas. Il faut généralement attendre très longtemps dans le cycle d'évolution de l'entreprise pour qu'un juriste entre dans l'entreprise. Ce vide n'est pas suffisamment comblé aujourd'hui par le conseil juridique des avocats ou des conseils. Nous voyons beaucoup de directeurs d'entreprise très intelligents, très diplômés, très capables qui, eux-mêmes, écrivent leurs contrats ou bataillent avec leurs partenaires. C'est bien sûr normal pour la partie commerciale ou économique mais ils sont personnellement à la manœuvre pour la rédaction du texte et ce n'est pas normal. Certains éléments du droit sont d'une extrême complexité, de plus en plus

complexes, ce qui signifie qu'ils peuvent oublier beaucoup de points sur les garanties, les indemnisations…

Nous sommes un peu sur une ligne de crête. Nous ne voulons pas être en infraction d'un point de vue réglementaire. Nous ne voulons pas être en porte à faux avec nos collègues et partenaires qui sont avocats et conseils. Nous voulons que l'entreprise ait une stratégie la plus fine, la plus forte et la plus pertinente possible. Il faut que les dirigeants d'entreprise s'en emparent et soient capables d'exprimer, vis-à-vis de leurs investisseurs, quelle est leur stratégie. Lorsqu'ils s'accaparent leur stratégie commerciale, marketing, certaines stratégies réglementaires, la stratégie de ressources humaines, de propriété intellectuelle et d'architecture juridique, cette stratégie doit être formalisée, comprise et exprimée par la direction.

M. Philippe Latombe, rapporteur. En comparant avec nos voisins anglo-saxons à l'ouest et nos voisins chinois à l'est, en comparant aussi au sein de l'Europe avec le tableau de bord européen de l'innovation, la France est dans la partie moyenne supérieure, parmi les innovateurs notables, mais pas dans le haut du classement parmi les champions de l'innovation. Qu'en pensez-vous ? Quelles bonnes pratiques pourrions-nous copier chez nos voisins européens ou généraliser en Europe pour devenir une véritable force d'innovation et pouvoir rivaliser avec nos voisins ?

M. Didier Patry, directeur général de France Brevets. Nous pouvons prendre la question sous plusieurs angles selon la façon d'interpréter les statistiques.

Un rapport de l'Office européen des brevets vient de sortir en décembre sur la quatrième révolution industrielle. Ce rapport comporte beaucoup de chiffres. Les auteurs se sont limités à des domaines très spécifiques tels que la collecte d'informations, le logiciel, la connectivité… Nous devons malheureusement constater qu'aucune entreprise française ne fait partie des 25 plus gros déposants au monde. Cette liste comporte des entreprises allemandes, néerlandaises mais pas d'entreprise française. *Les Échos* ont repris cette étude et noté le fait que la France est placée en troisième position en Europe mais il faut aussi regarder le nombre de dépôts de brevet par habitant. Nous sommes de ce point de vue en huitième position en Europe, juste devant l'Espagne et l'Italie. L'Allemagne est très loin devant : elle dépose entre deux et quatre fois plus de brevets que la France, toutes catégories confondues. La France est aussi tout simplement absente de certains classements ce qui est un sérieux problème.

Que faire ? C'est une vaste question. Notre programme de la Fabrique à brevets, tentait de réagir, avec nos moyens et surtout intelligemment, c'est-à-dire en ciblant au mieux. Globalement, lorsque nous n'avons pas toutes les munitions dont nous aurions besoin, la seule réponse est de faire un tir précis ou de s'échapper mais ce n'est pas ce que nous souhaitons faire. Nous voulons être à l'offensive. Nous devons donc cibler et calibrer au mieux ce dont l'entreprise a besoin. Notre réponse n'est pas dans le volume. Ce n'est pas possible.

Le moteur de recherche français qui, avec beaucoup d'ardeur, essaie actuellement de conquérir des parts de marché n'arrivera pas au volume de brevets du moteur de recherche américain que la plupart des gens utilisent. Le déséquilibre est d'un à mile, il est trop grand pour être rattrapé. Toutefois, par la qualité et un certain volume, nous pouvons tenter de remonter.

Ce volume n'a pas besoin d'être aussi grand que celui des Américains. Les chiffres américains sont généralement hors de proportion et c'est naturel puisque telle est culturellement leur façon de faire et qu'ils ont d'énormes moyens. La situation est d'ailleurs identique pour nos amis chinois. La réponse n'est certainement pas en essayant de copier ce

que font les autres mais nous pouvons essayer de nous rapprocher des modèles allemand ou suisse.

Je ne suis pas d'accord sur le fait que la propriété intellectuelle doive être *low cost*, qu'il faille rogner les taxes perçues par les offices. C'est un faux problème et le problème n'est pas dans les taxes. Le vrai problème est d'obtenir le retour le plus approprié pour chaque euro dépensé donc de choisir le bon conseil en propriété intellectuelle ou le bon avocat. Il faut aussi s'assurer que la collaboration soit forte, que le temps alloué au conseil pour la rédaction des demandes de brevet soit le plus grand possible avec un budget adéquat, pour aller vers la qualité. Je ne crois donc ni au *low cost* ni à une course aux chiffres.

Il nous faut cependant augmenter certains de nos chiffres. Comment le faire ? Peut-être devrions-nous observer ce que font les Allemands. L'acculturation à la propriété intellectuelle se fait très jeune, dès l'école primaire. De nombreuses écoles enseignent la propriété intellectuelle et l'incitation est forte pour les inventeurs, avec une rémunération beaucoup plus importante.

Nous faisons notre part, en essayant d'enseigner dans des universités, des écoles, des colloques. Nous essayons d'être présents et d'acculturer mais je pense qu'une réflexion au niveau de l'éducation nationale serait nécessaire pour amener vers une éducation plus forte à la propriété intellectuelle. Il faut le faire sans pudeur et je pense que c'est la première étape.

M. Philippe Latombe, rapporteur. Les Allemands déposent-ils beaucoup de brevets parce qu'ils développent beaucoup chez eux ? Vous disiez que nous devions avoir création de brevets à la fois par la R&D à l'intérieur de l'entreprise et par l'acquisition sur étagère. Les Allemands sont-ils aussi de forts acquéreurs sur étagère ? Ont-ils ces deux piliers ou privilégient-ils la création en interne ?

M. Didier Patry, directeur général de France Brevets. Nous n'avons malheureusement pas ces chiffres ; ce sont des analyses qui pourraient être faites. Notre regard se portait actuellement plus sur le côté ouest de l'Atlantique pour lequel nous avons des données que nous exploitons. Nous n'avons pas de données du côté allemand mais il faudrait effectivement aller observer la situation.

D'après les informations que j'ai du fait de mon passé dans l'entreprise et le monde industriel, les Allemands s'intéressent plus à la R&D interne car il existe de fortes incitations pour les inventeurs, avec à la clé une très forte rémunération en cas de succès de l'invention. La charge administrative imposée pour être capable de corréler tel brevet avec tel produit ou tel programme est d'ailleurs considérable pour les entreprises. Il s'agit de savoir si tel brevet de tel inventeur est à la source ou a contribué au succès d'un produit. C'est un énorme casse-tête administratif qui donne beaucoup de travail aux entreprises mais se traduit par le doublement du salaire de l'inventeur certaines années. C'est donc un très gros bonus qui incite à la R&D interne.

Les Allemands achètent aussi des entreprises et, en même temps qu'ils achètent une entreprise, ils acquièrent de la propriété intellectuelle.

Il ne nous semble pas intéressant d'entrer dans la guerre des volumes et de tenter de copier les Américains, les Allemands ou les Chinois. Même si la course n'est pas nécessairement perdue, elle risque de nous essouffler économiquement. Pour nous, la solution est aussi dans la structure systémique, c'est-à-dire dans une organisation intelligente des entreprises, par filière, pour que les entreprises définissent une stratégie commune de propriété

intellectuelle et y travaillent ensemble. C'est très novateur et peut apporter une plus grande efficacité sans dépenses ou sans dépenses complémentaires ou avec des dépenses très faibles.

Cela signifie concrètement que les entreprises se cotisent pour acheter des brevets : en se cotisant à dix pour acheter un brevet, chacun ne paie que 10 % du prix ce qui montre bien l'intérêt de l'opération. L'autre intérêt de cette opération est l'intelligence collective. Beaucoup d'entreprises ne sont pas au niveau de sophistication voulu et elles peuvent bénéficier des activités de leurs pairs lorsqu'elles communiquent avec eux. En offrant une plateforme de dialogue sur la stratégie de propriété intellectuelle aux chefs d'entreprises ou aux responsables au sein des entreprises, nous pouvons percoler, diffuser une vision stratégique vers les plus faibles et les plus petits.

Nous travaillons donc actuellement sur un programme de stratégie de filière, par filière, pour que les entreprises associent leurs moyens. Cette mutualisation offrira une dissuasion : les brevets acquis coûteront certes moins cher à chacun mais, surtout, ils apporteront un effet de dissuasion contre les agresseurs potentiels. Le fait d'être en groupe permettra un deuxième niveau de dissuasion puisqu'un groupe a moins de risques d'être agressé qu'une entreprise isolée.

Je ne suis donc pas sûr qu'il faille imiter ce que font les autres en ce qui concerne les volumes de brevets. Je pense que cette quête est un peu dangereuse comme nous l'avons vu récemment dans le cas d'une start-up française ayant une très belle technologie qui est allée manifestement beaucoup trop loin dans son volume de brevets, tellement loin qu'elle a fini par faire peser trop de coûts sur sa trésorerie et s'est retrouvée en très grande difficulté.

Nous proposons un programme d'alliances, de coalitions, de groupements. Nous y travaillons depuis plus d'un an et avons présenté ce programme aux différents cabinets, aux décideurs, aux cercles de décision et aux cercles industriels. Notre conseil d'administration a approuvé le lancement de ce projet. Il devrait donc être lancé en 2021. Ce projet est extrêmement novateur en France et en Europe. Il existe des initiatives similaires outre-Atlantique. Elles ont d'ailleurs fonctionné ce qui nous inspire beaucoup.

Cette réponse est à notre avis pertinente, pragmatique et peu coûteuse. Elle représentera pour les entreprises une fraction de ce qu'elles devraient payer pour déposer un seul brevet grâce à la mutualisation. Nous n'excluons pas le partage, pour ceux qui sont intéressés, de leurs propres brevets au profit de la communauté de la filière. Ceux qui le font bénéficieraient d'une diminution de leur cotisation et éventuellement d'une prise en charge de leurs frais de brevets par les cotisants de la filière. L'effet sera ainsi double : les membres de la filière profiteront de brevets qui ne sont pas les leurs et celui qui met ses brevets au pot commun verra ses coûts diminuer donc aura des charges moins importantes et pourra réinvestir dans l'économie ou dans sa propre R&D.

M. Philippe Latombe, rapporteur. Vous avez dit que les entreprises, actuellement, ne disposent pas forcément d'une structure juridique en interne ou n'ont pas le réflexe d'une structuration juridique en externe. Vous travaillez avec des conseillers pour les aider sur la partie brevets et avec des avocats pour la partie juridique. Vous êtes donc au cœur du système et voyez l'ensemble de la situation. Que pourrait faire la puissance publique pour vous donner plus de fluidité dans votre travail ? Pourrions-nous enlever rapidement certains grains de sable ? Existe-t-il des gros cailloux auxquels nous devons nous attaquer pour vous aider à moyen terme ?

M. Didier Patry, directeur général de France Brevets. L'important serait d'améliorer la collaboration entre les outils du PIA. Depuis une dizaine d'année, nous avons

tous appris et nous sommes aujourd'hui à un niveau d'expertise et de professionnalisme nettement plus élevés. Je pense que le moment est venu de nous demander comment articuler et coordonner au mieux tous ces outils.

Lorsque nous faisons la promotion d'un portefeuille de brevets de qualité, de taille suffisante au travers du programme de la Fabrique à brevets, nous incitons l'entreprise à acheter des brevets auprès de la recherche publique. Ces brevets peuvent se trouver dans les sociétés d'accélération du transfert de technologies (SATT) ou auprès d'instituts techniques, de laboratoires de recherche. Plus nous avons de visibilité sur les brevets disponibles sur les étagères, plus nous pourrons aller vite. Une collaboration entre ces organismes et nous-mêmes serait donc très intéressante.

Cela peut concerner le Centre national de la recherche scientifique (CNRS) et CNRS Innovation, l'Institut Pasteur ou l'Institut national de la santé et de la recherche médicale (Inserm) avec Inserm Transfert. Nous collaborons déjà, grâce à des relations personnelles ; nous nous croisons régulièrement mais je pense que, en augmentant cette collaboration, nous permettrons de mieux satisfaire les besoins de l'industrie française et d'avoir plus de fluidité dans la mécanique, à tous les niveaux.

Au niveau des institutions, nous avons actuellement un bon dialogue avec les cabinets et avec un certain nombre de députés ou de sénateurs. Nous avons beaucoup œuvré pour le plan d'action pour la croissance et la transformation des entreprises (loi PACTE) qui nous a semblé être une excellente proposition et que nous avons fortement soutenu. Nous avons bataillé en sa faveur et cela nous a permis de nouer des liens avec certains députés et des sénateurs. Cet échange extrêmement fructueux a également alimenté notre réflexion personnelle.

La collaboration est fondamentale et nous devons avoir une vision à 360 degrés. Cela peut être fait très rapidement, par exemple au sein du plan de relance dans lequel un ou des chefs de projet pourraient intégrer l'élément « propriété intellectuelle ». Nous collaborons avec France Stratégie qui est évidemment l'entreprise qui « met sur le radar », ce que pourrait être le futur, les risques et les opportunités. Toutes les informations doivent aller vers le plan de relance pour que, au sein du plan de relance, l'intégration des composantes de la propriété intellectuelle ait lieu aussi rapidement que possible, avec la mise en place de mesures correctives ou de plans de protection ou de parades. Nous proposons de créer ces parades dans le cadre d'une stratégie par filière. Ces parades peuvent être mises en œuvre immédiatement.

Il n'existe pas énormément de cailloux mais tout le monde est extraordinairement occupé, encore plus du fait de la pandémie puisqu'il y a urgence à sauver la France en quelque sorte, les PME et les artisans qui sont en très grande difficulté. La propriété intellectuelle n'est pas forcément la principale préoccupation et c'est tout à fait naturel.

Toutefois, en 2021, pour la relance, l'ambition n'est pas seulement de rester à genoux mais de se lever, de courir et si possible de gagner la course. Nous ne gagnerons la course que si nous avons des stratégies de propriété intellectuelle sophistiquées. Il ne s'agit pas seulement d'en avoir ; elles doivent être au plus haut niveau de sophistication car nos partenaires et parfois concurrents, à l'est ou à l'ouest, sont dans un très haut niveau de sophistication, dans une prise en compte et une intégration très précoce de la propriété intellectuelle et des brevets, avec des objectifs très nets. Ainsi, le plan d'expansion de la Chine cite la propriété intellectuelle et les brevets comme un levier pour cette expansion économique. C'est normal puisque c'est ce qu'ont fait nos amis d'outre-Atlantique. La Chine a tout à fait saisi cette philosophie et s'en inspire.

Plutôt que d'enlever des grains de sable, il s'agit donc de lancer un signal au plus haut niveau des institutions, des cabinets et des ministères, de dire que la propriété intellectuelle est importante, qu'il faut y penser, l'intégrer et l'intégrer avec des professionnels.

M. Philippe Latombe, rapporteur. La crise pandémique actuelle a un impact sur l'économie. Laissera-t-elle des traces ? Ne relèguera-t-elle pas l'ensemble du processus de brevets et de propriété intellectuelle au second plan s'il faut d'abord survivre économiquement ? Comment relancer la machine pour 2021 ?

M. Didier Patry, directeur général de France Brevets. Il y a effectivement urgence et tous les responsables – Bruno Le Maire, Agnès Pannier-Runacher, Cédric O – se sont très fortement mobilisés. Nous enregistrerons bien sûr des pertes malgré ce gros effort. Je n'ai pas l'impression que la propriété intellectuelle soit négligée même si elle n'est pas citée immédiatement. Nous sommes un peu négligés dans l'urgence mais c'est naturel et nous ne pouvons rien y faire.

Toutefois, il faut s'assurer que l'argent mis sur la table se transforme rapidement en valeur. Ce ne sera pas simple mais il se produit une prise de conscience intéressante, visible dans des expressions telles que « souveraineté ».

La souveraineté est pour nous l'indépendance opérationnelle, le droit de choisir entre une entreprise française et une entreprise d'un autre pays. Je crois que nous allons dans le sens de cette indépendance opérationnelle. La pandémie a eu pour vertu de faire apparaître cet élément.

Vous et moi communiquons aujourd'hui sur une plateforme de visioconférence qui n'est pas européenne. Je crois que l'ordinateur que j'utilise actuellement n'est pas de marque européenne pas plus que le téléphone à côté de moi, le logiciel que nous utilisons ou la majorité des composants électroniques de mon ordinateur. Nous l'avons compris et je pense qu'un réveil a lieu.

Nous voyons déjà dans le *Digital Services Act* (DSA) et le *Digital Market Act* (DMA) un travail collectif de la Commission européenne et des États membres en faveur d'une idée de *Europe first* ou de *France first*. Je pense que c'est important et nous amènera à réfléchir à la souveraineté, à l'autonomie et à l'indépendance opérationnelle. Cela signifie avoir des entreprises viables, qui survivent et grandissent.

Que faisons-nous pour rééquilibrer les rapports de force très déséquilibrés entre nos entreprises et les entreprises étrangères ? Les cadres des marchés sont parfois un coupe-gorge pour nos entreprises, surtout outre-Atlantique où des entreprises se sont fait agresser localement, au tribunal, avec des coûts énormes – 4 à 6 millions de frais d'avocats par an que l'entreprise ne récupère pas, même si elle gagne – et donc un impact très important sur la marge opérationnelle.

Une entreprise ne survit pas sans marge. Il est donc impératif que les entreprises préservent leur marge. La marge sur un véhicule ou sur une batterie est très faible, de l'ordre du pourcent. Ce n'est pas comme lorsque je me fais un café : les capsules de café font actuellement environ 80 % de marge. Sur un véhicule, l'entreprise est au pourcent près. Si elle doit payer des frais de licence à des entreprises externes parce qu'elle ne dispose pas de la technologie et des brevets nécessaires, cela posera problème.

Cette autonomie opérationnelle ne pourra donc être acquise que lorsque nous aurons un choix local, la liberté de choisir, ce pour quoi il faut encore avoir des entreprises à choisir !

Si nous ne parvenons pas à protéger nos entreprises lorsqu'elles sont mises à mal à l'étranger par une organisation systémique en France, nous n'aurons pas d'autonomie parce que nous n'aurons pas d'entreprise.

M. Philippe Latombe, rapporteur. J'essaie de réfléchir aussi à l'avenir à moyen et long terme. L'intelligence artificielle se développe fortement et nous pouvons envisager qu'elle devienne créatrice de contenus brevetables ou pouvant faire partie de ces actifs immatériels. Nous n'avons pas réfléchi jusqu'à présent à la structure juridique qui accompagnerait de tels développements. Nous ne savons pas qui deviendrait le créateur ou le propriétaire. Avez-vous réfléchi à ces questions ? Pensez-vous qu'il existe d'autres sujets sur lesquels nous devrons nous pencher à un moment ou un autre, sur lesquels vous souhaitez attirer notre attention pour que nous y réfléchissions aussi ?

Le débat monte dans la communauté juridique pour savoir s'il faut donner une personnalité à l'intelligence artificielle ou non, si elle est un mineur sous tutelle ou rien du tout. Voyez-vous d'autres sujets dans votre champ de travail auxquels nous devons commencer à réfléchir ?

M. Didier Patry, directeur général de France Brevets. De nombreux débats ont eu lieu sur l'intelligence artificielle, en particulier pour savoir si une invention issue d'une intelligence artificielle est brevetable. Beaucoup d'encre coule dans ce domaine et des décisions ont déjà été prises. Je ne pense pas que nous ayons besoin d'y réfléchir. Nous pouvons y contribuer mais beaucoup de gens y réfléchissent déjà. Il ne me paraît pas nécessaire que nous ajoutions notre grain de sel à un domaine déjà très salé.

Il me semble par contre utile de rappeler quelques fondamentaux. Tout d'abord, le logiciel est brevetable et il est breveté massivement. Environ 70 % des brevets délivrés aujourd'hui aux États-Unis, toutes catégories confondues, sont des brevets de logiciels. Les Américains ont donc largement bétonné leur territoire économique de prédilection. En Europe, nous avons toujours un courant de pensée selon lequel le logiciel n'est pas brevetable. Pourtant, il l'est même si le taux de réussite au contentieux sur les brevets de logiciels n'est pas très important. De nombreuses sociétés déposent, malgré tout, des brevets dans le domaine logiciel, y compris dans celui de l'intelligence artificielle qui s'exprime *in fine*, d'un point de vue technologique, par un logiciel.

Certains croient que le logiciel libre, *open source*, serait la réponse européenne pour éviter les mécanismes de dépendance extrême dans lesquels nous sommes. Nous sommes loin de la souveraineté numérique, nous sommes inféodés. Le logiciel libre n'est pas la réponse parce qu'il n'est pas immunisé vis-à-vis des brevets de tiers. Tout le monde ne l'a pas bien compris aujourd'hui. Le logiciel libre est immunisé vis-à-vis de ceux qui contribuent mais pas vis-à-vis de ceux qui n'y contribuent pas. C'est d'ailleurs la raison pour laquelle une grande société de la côte Est a eu un programme de licence extrêmement agressif vis-à-vis d'Android, pourtant logiciel libre.

Il faut faire attention à ces croyances, à ces dogmes, savoir raison garder et faire une analyse calme et sereine. Nous ne devons pas avoir des croyances religieuses mais être capables de comprendre les mécanismes, les avantages et les inconvénients et où nous pouvons réussir.

À mon avis, nous pouvons réussir dans un modèle propriétaire. Nous pouvons aussi réussir dans un modèle de logiciel libre mais à condition de très bien savoir comment manier ce modèle qui est dangereux et potentiellement très toxique. Peut-être serait-il utile d'établir une doctrine vis-à-vis du logiciel libre, ses limites, les précautions à prendre pour que nous ne

soyons plus dans le dogme, l'incantation ou la croyance religieuse mais dans l'analyse et le rationnel.

Un autre élément, peut-être moins important, sans rapport avec l'intelligence artificielle et le logiciel ou la brevetabilité, est la question des moyens juridiques, techniques, systémiques utilisables pour être plus forts, en France et en Europe.

Je pense que nous devrions continuer à travailler sur le droit de la concurrence car c'est le droit qui s'est montré le plus coercitif, dans ce pays et en Europe en général. Nous devrions nous demander comment régler les situations de déséquilibre et les utilisations abusives de la propriété intellectuelle ou des systèmes juridiques hors de nos frontières pour mener des actions de prédation ou de déstabilisation contre nos entreprises. Le droit de la concurrence ne peut-il pas rééquilibrer ces situations de déséquilibre et d'abus en dehors de nos frontières ? Nous nous posons la question et travaillerons certainement dessus, bien que la ligne soit assez fine.

Cette question nous semble importante car l'extraterritorialité n'existe que parce que notre système juridique est faible, que nous ne voulons pas nous opposer à ces actions d'extraterritorialité. Il faut que nous revoyions notre copie et que nous réfléchissions à la façon dont la solidité de notre système juridique national, sa pertinence et son impact pourraient aider nos entreprises. Il faut donner des moyens au système, aux tribunaux. Il faut que les juges disposent de moyens et de temps, puissent prendre le temps de décider de façon professionnelle. Notre justice a besoin de moyens pour être efficace. Ce n'est malheureusement pas toujours le cas et nos entreprises ne peuvent pas se reposer sur notre système. C'est un réel problème qui rend trop facile l'utilisation de mécanismes d'extraterritorialité du fait de l'absence de défense et de protection chez nous.

M. Philippe Latombe, rapporteur. Pensez-vous que le DSA et le DMA peuvent y contribuer par leur volet consacré à la transparence dans la concurrence ? Est-ce un embryon qui va dans le bon sens, qu'il faut que nous appuyions encore ou sommes-nous passés à côté ?

M. Didier Patry, directeur général de France Brevets. Ces textes sont le signal que l'Europe veut s'organiser et c'est fondamental. Ces documents contiennent beaucoup d'intelligence ; ils sont denses, épais, complexes. Ils témoignent de beaucoup de réflexion et n'ont pas été rédigés à la va-vite ; nous pouvons en être fiers.

Le sujet principal de ces documents n'est pas la propriété intellectuelle et certains regrettaient d'ailleurs le manque de mesures liées à la propriété intellectuelle. Je pense que ce n'était pas l'objet. L'objet était d'amener dans l'espace numérique des règles de droit qui sont celles du sol, de notre espace, de faire en sorte que nous ne soyons pas dans le Far-West mais plutôt dans un espace réglementé avec une protection des consommateurs, la capacité de rejeter des contenus haineux… Je pense que le signal ainsi lancé va vraiment dans la bonne direction par l'organisation mise sur pied mais il faut évidemment aller plus loin.

La transparence est fondamentale. Le sujet qui nous touche parfois est la transparence des programmes de licences liés aux brevets essentiels aux normes. Ce sujet reviendra nous toucher puisque, pour la 5G par exemple, la France a contribué mais les plus gros contributeurs sont chinois ou américains. Les quelques contributeurs européens souhaitent tout naturellement administrer les programmes de licences qui s'appliqueront aux entreprises montant des réseaux 5G privés. C'est compliqué par manque de transparence dans cette mécanique. Nous ne savons jamais vraiment qui paie combien.

Des initiatives ont eu lieu récemment dans l'automobile pour clarifier la tarification, ce qui n'a pas forcément donné des résultats positifs car une très grande société européenne de télécommunications est maintenant en conflit direct avec une très grosse société allemande de l'automobile. Ce procès fait beaucoup parler de lui. La tarification forfaitaire n'a donc pas apporté de réponse. Il faut faire encore des efforts de transparence pour que nous ayons tous des informations sur les prix pratiqués. Tout le monde a à y gagner.

Les DSA et DMA ne contiennent donc pas grand-chose sur les brevets et la propriété intellectuelle mais ils vont dans le bon sens et ils sont importants car ils donnent un axe à l'Europe. C'est fondamental et cela signifie que l'Europe veut compter dans l'espace du numérique. Nous nous en réjouissons.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder d'autres sujets ?

M. Guillaume Ménage, directeur adjoint de France Brevets. Je voudrais insister sur deux points. L'innovation et sa protection nécessiteront toujours des fonds, des capitaux, des investissements.

La première étape est la culture qui peut passer en particulier par la formation. Nous intervenons dans différents modules mais, si vous regardez d'où vient l'innovation c'est-à-dire les gens qui ont un parcours d'ingénieur et de management, ces personnes ont suivi très peu de modules de formation sur la propriété intellectuelle. La formation ne doit pas être une formation d'expert mais elle doit générer un réflexe. Nous avons des experts, des juristes et des avocats spécialisés en propriété intellectuelle. La personne qui innove doit toutefois savoir que l'étape qui suit immédiatement l'innovation est la protection. Nous insistons pour intégrer la formation sur la propriété intellectuelle au plus tôt dans les écoles d'ingénieur, de management et autres. Ce point nous paraît fondamental pour créer une culture dans le pays.

Mon deuxième point concerne les grands projets nationaux et européens pour pousser de nouvelles innovations, de nouvelles technologies et qui doivent être accompagnés d'une politique de propriété intellectuelle, autrement dit d'une doctrine de propriété intellectuelle. Nous voyons des projets mis en place avec des subventions mais un programme autour de la propriété intellectuelle faible voire inexistant. France Brevets est à disposition pour y contribuer. Nous avons tous en tête que le niveau élevé de militarisation de l'économie dans d'autres pays et la façon dont ils abordent notre marché nécessitent que nous ayons cette dimension et cette doctrine, que nous agissions tous ensemble.

M. Philippe Latombe, rapporteur. Cette question de l'éducation ressort effectivement d'autres auditions que nous avons déjà menées. Nous avons un levier important à mettre en place dans les écoles d'ingénieur, de management et même plus tôt au sein de l'éducation nationale, au collège et au lycée. Le rapport contiendra un gros volet sur l'éducation, à la fois sur votre domaine et sur d'autres sujets connexes.

M. Didier Patry, directeur général de France Brevets. J'insiste aussi sur le fait que la France a été à l'origine de grandes évolutions législatives dans le domaine de la propriété intellectuelle. Au niveau international, la France est à l'origine de la convention de Paris sur la propriété intellectuelle de 1883. Elle est fondamentale dans la structuration de la propriété intellectuelle et du droit d'auteur dans le monde. La France est très active dans le domaine des marques mais pas suffisamment dans le domaine des brevets.

Il nous semble important de communiquer aux élèves des écoles d'ingénieur, de commerce, de stratégie et de management ou même de sciences politiques des recettes stratégiques. Nous ne souhaitons pas faire de ces gens des juristes. Ils peuvent le devenir s'ils

le souhaitent et il existe dans ce domaine des formations très nobles, riches et intellectuellement intéressantes, qui forment l'esprit ; c'est d'ailleurs la raison pour laquelle beaucoup d'Américains font des études de droit en plus de leurs études d'ingénieur ou de commerce. Ceci étant, il est important que tous aient rapidement une idée de la stratégie à prendre, qu'ils aient des réflexes, qu'ils puissent s'accaparer et se former une vision stratégique. Cela ne nécessite pas un master mais simplement la mise en place de modules avec de bons intervenants. Nous avons ces intervenants en France et il faut que les directions des écoles prennent conscience que cette formation est importante. Ce ne sont pas des investissements énormes.

Nous venons tous et toutes du privé, avec un bagage provenant de différentes entreprises nationales ou internationales. Toutes nos observations sont le fruit d'années d'expérience. Ce qui importe est finalement le futur économique de la France, son indépendance économique. Il s'agit de faire en sorte que, demain, nos enfants, nos familles et nos voisins trouvent un emploi de qualité, qui permette au pays non seulement de survivre mais de vivre bien. Qu'on le veuille ou non, toutes les économies qui vivent bien, toutes les entreprises qui réussissent ont intégré très tôt la propriété intellectuelle et les brevets, de façon forte, au niveau le plus élevé de la direction et avec des moyens importants. Nous ne pourrons pas y échapper. Ce n'est pas une option.

Nous vous remercions de nous donner cette possibilité de nous exprimer. La France a beaucoup de capacités, beaucoup de gens très intelligents, très forts, très bien formés. Ce n'est qu'une question de transformation et d'articulation. Ce n'est pas très compliqué mais il faut le vouloir et le faire.

M. Philippe Latombe, rapporteur. L'objectif de cette audition était effectivement de savoir, grâce à votre expérience, ce qui marche et ne marche pas. Je vous remercie du temps que vous nous avez consacré. Cette audition était très intéressante et enrichissante.

Audition, ouverte à la presse, de M. Denis Psomiades, président-directeur général de la Compagnie lyonnaise d'études et de services en systèmes électroniques (CLESSE)
(17 décembre 2020)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous auditionnons ce matin le président-directeur général de la Compagnie lyonnaise d'études et de services en systèmes électroniques (CLESSE), M. Denis Psomiades. La CLESSE est une petite et moyenne entreprise (PME) lyonnaise, spécialisée depuis trente-cinq ans dans le pilotage des moteurs électriques, qui a également développé une gamme d'ordinateurs nommés Business Computer, conçus et fabriqués à 100 % en France.

Nous vous entendons dans le cadre des réflexions de la mission sur la souveraineté numérique et technologique de la France et de l'Union européenne. Votre audition préludera utilement aux différentes tables rondes relatives à la commande publique que nous prévoyons d'organiser en janvier.

Je souhaite que vous nous présentiez votre entreprise, que vous nous fassiez part de votre regard sur la notion de souveraineté numérique. Je crois qu'elle n'est pas définie tout à fait de la même manière dans les différents pays européens. Je voudrais avoir votre avis sur la meilleure façon, pour les pouvoirs publics, de promouvoir cette souveraineté.

Nous écouterons avec beaucoup d'attention une courte présentation du marché des ordinateurs sur lequel vous êtes présent en France si vous souhaitez nous en faire une. Nous aimerions aussi connaître votre actualité pour 2021 et la façon dont la pandémie a pu impacter vos activités en 2020.

M. Philippe Latombe, rapporteur. Je me réjouis que nous auditionnions le dirigeant d'une PME qui propose une gamme d'ordinateurs conçus et fabriqués en France à 100 %. Nous avons en effet à cœur de rencontrer des acteurs privés développant des solutions technologiques souveraines afin qu'ils partagent avec nous leur regard de praticien sur le sujet.

Je voudrais d'abord savoir quel sens revêt pour vous la notion de souveraineté numérique. Ce concept, parfois rapproché de celui d'autonomie, désigne une forme d'indépendance, de capacité à maîtriser son destin numérique et à ne pas subir les contraintes imposées soit par des acteurs publics comme les États soit par des acteurs privés comme les géants du web (GAFAM). Je voudrais savoir ce que vous pensez de la montée en puissance de cette thématique dans le débat public.

Il me semble également intéressant que vous nous indiquiez de quelle façon cet enjeu impacte votre activité en tant qu'entreprise développant une gamme d'ordinateurs autonome sur le plan technologique.

J'aimerais aussi revenir avec vous sur la façon dont les pouvoirs publics français ou européens peuvent concourir à promouvoir ou à protéger notre souveraineté numérique. Nous avons en effet auditionné des collectivités locales avec lesquelles nous avons abordé les enjeux de la commande publique. À votre échelle, qu'attendez-vous des acteurs publics ? L'accès à la commande publique vous semble-t-il suffisant ? Nous sommes évidemment intéressés, le cas échéant, par les pistes de recommandations que vous pourriez nous suggérer sur ce point.

Enfin, nos travaux portent aussi sur la dimension technologique de la souveraineté numérique, qui est au cœur du plan de relance présenté par le Gouvernement. Je souhaite que vous nous fassiez connaître le regard que vous portez sur l'action des pouvoirs publics, aussi bien sur la partie du financement que sur la protection des savoir-faire d'une entreprise technologique. J'aimerais aussi que nous ayons un échange sur les secteurs technologiques au sein desquels il est selon vous indispensable de développer une autonomie afin d'éviter d'éventuelles ruptures d'approvisionnement en composants stratégiques en cas de crise. L'expérience de la crise de la covid pourra peut-être utilement nous éclairer.

M. Denis Psomiades, président-directeur général de CLESSE. Je vais vous répondre en trois temps, en expliquant d'abord pourquoi nous ne faisons actuellement pas de souveraineté numérique, ensuite comment il est difficile de se protéger dans le magma actuel des solutions proposées et enfin en détaillant les difficultés que nous rencontrons en essayant de faire de la souveraineté numérique.

CLESSE conçoit et fabrique depuis trente-cinq ans des équipements électroniques industriels et, depuis l'année dernière, un ordinateur 100 % français. Je tiens à m'excuser par avance pour les raccourcis que je devrai faire : le sujet très vaste et je serai donc succinct sur certains points.

Pourquoi s'intéresser à la souveraineté numérique ? Bernard Benhamou, secrétaire général de l'Institut de la souveraineté numérique, écrit : « *Nous devenons vulnérables parce que nous sommes obligés d'avoir recours à du code que nous n'avons pas créé. Ce code est porteur de valeurs et de principes qui ne sont pas les nôtres, tant en termes de protection des données personnelles qu'en termes d'organisation du dialogue social ou d'évolution de nos sociétés*. » Le tableau est posé et la situation paraît très grave. Je note en particulier dans cette phrase les termes « vulnérables » et « obligés ». Il semblerait donc que notre vulnérabilité provienne d'une obligation, que nous n'ayons aucun moyen d'action.

Je prends quelques exemples concrets. Lise Charmel, société lyonnaise qui confectionne de la lingerie féminine, est aujourd'hui en redressement judiciaire à la suite d'une attaque par rançongiciel. Du fait que nous ne sommes pas souverains, cette société utilise un outil, en l'occurrence des ordinateurs, qui sont manifestement critiques pour son fonctionnement puisque c'est à la suite du rançongiciel qu'elle s'est retrouvée en redressement judiciaire. Ces outils ont été conçus par des gens qui n'ont pas les mêmes intérêts que nous. Si nous considérons n'avoir aucune solution alternative, les sociétés françaises sont condamnées, comme Lise Charmel, à être vulnérables aux rançongiciels. C'est un constat qui pose problème puisque cela commence à impacter nos sociétés. La confection, donc la mode, touche la société de manière générale et notre propre vision de l'avenir, de la vie et de la façon de vivre en France.

Mon deuxième exemple est le cas de la société Saint-Gobain qui a été un jour attaquée par un rançongiciel. Selon leurs publications, cela leur aurait coûté 250 millions d'euros. C'est un très gros chiffre que je veux mettre en rapport avec une étude universitaire selon laquelle réaliser un système d'exploitation (OS, *operating system*) coûterait environ 800 millions d'euros. Trois attaques de Saint-Gobain permettraient en gros de payer un système d'exploitation français donc souverain. Je ne suis pas vraiment d'accord avec le calcul qui suit dans l'étude universitaire, indiquant que cela coûterait 12 euros par Français et ne serait donc économiquement pas rentable. Il faut savoir que les coûts informatiques dans une entreprise, en prenant tout en compte, sont de 2 000 à 5 000 euros par poste et par an. L'universitaire ajoute que le gouvernement français aurait des ambitions de souveraineté en matière de système d'exploitation, que ce n'est pas bien et que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) n'est heureusement pas d'accord.

Les grandes entreprises changent actuellement en moyenne un quart de leur parc informatique chaque année, de façon à le renouveler entièrement tous les quatre ans pour suivre l'évolution du matériel et des systèmes d'exploitation. En matière d'obsolescence programmée, je pense que ce domaine est quand même un peu sur le podium, surtout que nous savons aujourd'hui qu'il n'est pas nécessaire de faire évoluer ainsi les systèmes d'exploitation dans les entreprises.

Je passe à un autre exemple : dans une conférence disponible sur le site du Club de la sécurité des systèmes d'information régional (CLUSIR), un club de directeurs des systèmes d'information (DSI) lyonnais, présentée en partie par une représentante de la caisse primaire d'assurance maladie (CPAM), se trouve une liste non exhaustive des difficultés rencontrées par le service informatique de la CPAM, dont l'évolution non souhaitée des systèmes d'exploitation. L'un des exemples présentés est le fait qu'il est demandé à un certain nombre d'agents de venir un samedi pour rattraper un retard dans le traitement des dossiers occasionné par une surcharge de travail. Lorsqu'ils arrivent le samedi, le système d'exploitation se met à jour ce qui leur fait déjà perdre vingt minutes et, ensuite, l'outil logiciel qu'ils devaient utiliser n'est plus disponible après la mise à jour du système d'exploitation. Ce sont des coûts dont on parle rarement, beaucoup moins que des rançongiciels qui sont des accidents. Cet exemple n'est pas un accident, c'est un coût récurrent qui impacte les administrations et pas seulement. De ce fait, les entreprises ne peuvent pas atteindre le meilleur de leur performance. Les coûts entraînés par un tel phénomène, qui engendrent de plus des coûts de maintenance, sont liés uniquement à une évolution du matériel, et même ici uniquement du système d'exploitation, qui n'est pas souhaitée.

J'ai un dernier exemple très concret, celui de mon boulanger qui m'a dit ne détenir absolument aucune information confidentielle ou stratégique. Un jour, il passe par mail à son fournisseur de farine des commandes plus importantes que celles qu'il fait d'habitude pour une raison quelconque qui fait qu'il a vendu plus de pain que d'habitude. Il se trouve que tous les boulangers en Europe ont vendu plus que d'habitude et donc rachètent plus de farine. Ils envoient tous par mail des commandes à leurs fournisseurs. Nous voyons alors l'expression concrète du *big data* : il existe des sociétés dont le métier est de récupérer des informations anonymisées, de les traiter, d'en tirer des tendances et d'acheter des actions sur les marchés pour faire des gains financiers avant même que le travail ait été fait par le fournisseur et l'acheteur. Cette capacité à intervenir sur le marché du blé en l'occurrence et donc à en tirer des profits sur notre dos avant même que le travail ait été fait est un préjudice difficile à apprécier mais qui est réel quotidiennement, aujourd'hui, tant que nous n'avons pas la capacité de protéger la totalité de nos données, y compris celles de mon boulanger.

Voilà pourquoi il est nécessaire d'être souverain sur la totalité des données. La perte de souveraineté constitue du piratage et du sabotage d'entreprises. Le rançongiciel est du piratage lorsqu'il se contente de demander de l'argent et devient du sabotage lorsque nous ne parvenons pas à avoir les codes de déchiffrement. De plus, si le chiffrement était dormant depuis six mois, même les sauvegardes sont corrompues d'où des problèmes pour les entreprises. C'est même parfois un assassinat lorsque les gens impactés se suicident. Ce n'est pas moi qui le dis mais une source de la gendarmerie nationale l'explique très clairement et ce n'est pas anecdotique. C'est donc très grave.

Comment se fait-il que, après cinquante ans d'informatique, nous en soyons toujours à avoir des problèmes de ce type ? Il est tout de même étonnant que nous ne parvenions pas à sécuriser les ordinateurs que nous utilisons. Il faut bien comprendre que, dans un ordinateur, tout passe par le système d'exploitation. Aucun logiciel ne peut fonctionner sans que les entrées et sorties de ce logiciel passent par le système d'exploitation : le clavier, l'ethernet

donc internet, la souris, l'écran… Le code secret que vous tapez pour chiffrer un fichier que vous voulez sécuriser passe par le clavier donc par l'OS qui prend le code pour le donner à votre logiciel de chiffrement. Même lorsque vous installez un logiciel, c'est en fait le système d'exploitation qui installe le logiciel comme il a envie de l'installer.

Le problème est que les OS contiennent des portes dérobées – *back doors* – et des failles. Nous en découvrons régulièrement dans tous les OS. Vous devez donc avoir une entière confiance dans celui qui a fait l'OS et dans l'OS lui-même.

Or, aujourd'hui, ceux qui ont fait les OS n'ont pas les mêmes intérêts que nous. Ils défendent leur propre pouvoir d'achat, le pouvoir d'achat de leur pays, leur culture et tout le reste. Parfois, certains disent que les emplois qui en découlent nous permettent de travailler. Le problème est que ce sont des emplois précaires, pauvres, parce qu'ils dépendent de modifications non souhaitées qui provoquent des coûts de maintenance chez nous. Ces coûts de maintenance sont totalement dépendants du bon vouloir de ceux qui font les modifications des systèmes d'exploitation. Les entreprises françaises ont ainsi décidé de changer un quart de leur parc informatique chaque année et nous voyons bien le coût que représente le fait de changer un quart du parc alors qu'il n'y en a pas besoin fondamentalement.

Il existera donc toujours un différentiel de productivité entre les concepteurs des systèmes d'exploitation et ceux qui se contentent de les utiliser. Ce différentiel de productivité nous met toujours en difficulté commercialement.

Lorsque les amortisseurs d'une voiture sont fatigués, que faut-il faire ? Changer toutes les routes de France, les élargir, mettre des barrières pour que cette voiture puisse rouler ? Vaut-il mieux changer les amortisseurs de la voiture ? Aujourd'hui, la meilleure solution serait d'avoir un ordinateur de confiance qui permettrait d'éviter toute cette charge.

Actuellement, environ 60 000 personnes travaillent dans la cybersécurité en France. Ces 60 000 personnes dans la cybersécurité ne produisent rien, c'est une charge pour les entreprises, pour toutes les entreprises françaises et européennes. Pourtant, lorsque nous posons la question à un directeur des services informatiques (DSI), il répond qu'il n'existe pas d'alternative. Il a raison, il n'existe pas d'alternative et nous retrouvons ce que dit Bernard Benhamou : « *nous sommes obligés* ».

Nous avons proposé une alternative. Nous sommes français et nous avons les mêmes intérêts que tous les Français. Nous avons conçu un « *hardware* », un OS et des logiciels. Nous avons vendu le tout à des industriels de la région lyonnaise pour démontrer la faisabilité. En effet, lorsque nous avons dit que nous pouvions le faire voici six ans, personne ne nous a crus, en particulier pas la Banque publique d'investissement (BPI). Nous avons donc décidé d'investir sur fonds propres en comprenant que, tant que nous n'aurions pas démontré la faisabilité, il serait impossible d'en parler. Il existe ainsi aujourd'hui des entreprises qui fonctionnent quotidiennement avec des systèmes 100 % français.

Nous avons proposé le Business Computer à des DSI de grandes entreprises et à des administrations, dans le but de faire baisser le coût de la facture informatique de façon générale. Nous avons alors rencontré ce que nous appelons le « syndrome du DSI ». De quoi s'agit-il ?

Lorsqu'un directeur général (DG) d'une entreprise parle à son directeur commercial, il utilise des termes tels que « marge », « part de marché » que tout le monde connaît ce qui leur permet de se comprendre. Lorsqu'un DG parle à un DSI, le problème est qu'ils ne parlent pas du tout la même langue. Le DSI parle de machine virtuelle, d'architecture trois tiers, de VPN,

d'agrégateur de liens, de noyau… et le DG, ne comprenant même pas la langue, donne à son DSI l'entière responsabilité de la gestion informatique de l'entreprise. Comme le DSI est responsable de tout du fait que personne ne comprend ce qu'il fait, il choisit des solutions standard pour que, en cas de problème, il ne lui soit pas reproché d'avoir utilisé autre chose, tout en connaissant parfaitement les risques encourus.

Lorsque nous nous adressons à un DSI pour lui proposer un système de confiance français, la phrase que nous entendons systématiquement est : « *Je ne peux pas introduire dans mon entreprise un matériel atypique car, au moindre problème, je prendrais le risque de me faire licencier.* » Les choix en matière de souveraineté numérique ne sont donc pas guidés par les intérêts des entreprises mais par un problème d'habitude, peut-être parfois un manque de compétences compréhensible car l'informatique est un domaine très compliqué.

Si les directeurs généraux étaient conscients des risques, toute une part de la numérisation des entreprises ne se ferait pas. Par exemple, nous voyons aujourd'hui dans les entreprises des broyeurs de documents ; toute l'information est dans le *cloud* ce qui est une incohérence totale, donne un faux sentiment de sécurité aux gens et rend encore plus dangereuse l'utilisation de l'informatique dans certains cas de figure.

Nous en avons conclu que c'était aux institutions que revenait la charge d'aider les différentes composantes de la société à jouer collectif sur le sujet, à cautionner des solutions informatiques françaises comme le gouvernement américain l'a fait pour IBM, Facebook, Google et Amazon. C'est tous ensemble que nous pouvons renverser la tendance.

Nous avons donc contacté un ministère pour proposer notre Business Computer. Nous avons été mis en relation avec le responsable informatique du ministère qui m'a répondu ne pas pouvoir acheter un système français pour équiper son ministère s'il n'est pas certifié par l'ANSSI. Nous retombons donc sur le syndrome du DSI qui veut du matériel standard, certifié et ne le fait sinon pas rentrer dans l'entreprise. Nous ne pouvons donc pas créer en France une solution informatique innovante puisque l'ANSSI demande de faire un gros chiffre d'affaires pour accepter d'ouvrir un dossier de certification et que, pour faire un gros chiffre d'affaires, il faut être certifié. Il n'est pas possible d'entrer dans le système.

J'ai évoqué auprès de ce fonctionnaire du ministère le décret n° 2018-1225 qui permet à l'administration d'acheter une start-up hors cadre des marchés publics pour réaliser une preuve de concept. Ce décret tombe à pic ; il est très bien fait et permet de lever une barrière technique qui a sa justification puisque le code des marchés publics est très utile également. Le responsable informatique du ministère m'a répondu : « Ce n'est pas mon problème ! » Si ce n'est pas le problème de celui qui décide sous la tutelle du veto de l'ANSSI, il n'est pas possible aujourd'hui, en France, de proposer une véritable souveraineté numérique, du fait des institutions.

Il est clair que l'informaticien et l'ANSSI ne doivent pas détenir un pouvoir de veto sur le déploiement de solutions innovantes, françaises et, en définitive, favoriser en creux le déploiement de solutions étrangères qui ne sont pas plus certifiées et pas certifiables. C'était le sens du décret, décret que personne ne met en œuvre. Le simple fait que la solution soit française devrait au minimum susciter de l'intérêt et ce n'est pas le cas.

Nous n'en sommes pas restés là. Nous avons un client dans le secteur de la dissuasion nucléaire. Je vous rappelle qu'il s'agit de bombes atomiques et de missiles. Ce client est audité régulièrement par l'ANSSI. Nous lui avons proposé notre matériel. Il nous a répondu, selon le même syndrome du DSI, qu'il ne peut pas proposer nos produits à sa direction ni à ses clients parce qu'il a peur que l'ANSSI ne certifie pas leur système s'il contient nos solutions. Cela

signifie que, aujourd'hui, en France, nous utilisons pour la dissuasion nucléaire française des systèmes étrangers, pas certifiables du tout puisque nous n'avons pas accès aux sources des programmes, et que, pour faire de la bureautique dans les ministères, un système français qui pourtant serait certifiable n'est pas accepté. Je vous laisse seuls juges.

La doctrine de l'ANSSI n'est actuellement pas compatible avec le déploiement de solutions innovantes de sécurité françaises. L'ANSSI dispose d'un pouvoir de décision sur des choix de marchés stratégiques sur lesquels la France doit concentrer ses efforts. Or, ce type de choix ne fait pas partie des compétences des informaticiens. Ils ne sont pas formés pour. La doctrine de l'ANSSI consistant à dire que les Américains ont trop d'avance et donc que c'est peine perdue d'essayer de prendre des parts de marché dans le secteur des ordinateurs souverains est une erreur stratégique grave pour la France et l'Europe. Vous ne pouvez pas dire aux Français et à des chefs d'entreprise que nous abandonnons avant même d'avoir essayé la conquête d'un marché européen de 200 à 300 milliards d'euros. C'est tout simplement inaudible.

Tout ceci contraste avec la volonté manifeste de souveraineté du Président de la République dans pratiquement tous ses discours. Cela contraste également avec les injonctions de Bruno Le Maire envers les entreprises auxquelles il demande en substance de faire comme les grandes entreprises étrangères qui rencontrent un grand succès. Comment faire, puisque toutes les entreprises françaises partent avec un handicap que l'ANSSI, par idéologie, ne cherche pas à combler ?

Il faut comprendre que le système d'exploitation et le « *hardware* » sont la clé de voûte de toute la filière. Beaucoup de chefs d'entreprise en France l'ont très bien compris. Le Collectif des 200 qui s'est créé le crie haut et fort. La suprématie américaine s'est créée par exemple parce que les fabricants d'OS ont choisi des puces électroniques américaines pour équiper les ordinateurs américains. Si nous créons demain en France une véritable filière d'informatique souveraine, nous pourrons choisir par exemple des composants de STMicroelectronics ce qui lui permettra de faire beaucoup plus de chiffre d'affaires. Grâce à ce chiffre d'affaires, peut-être STMicroelectronics auraient-il pu avoir les moyens de racheter ARM, ce qui n'a pas été le cas. C'est ainsi que fonctionne une filière. En partant de l'ordinateur et de l'OS, nous finançons toute la filière.

En concevant vous-même un OS, vous avez six mois d'avance sur tous les autres développeurs qui l'utilisent. C'est ce qui a permis aux Américains de proposer dans des solutions standards du marché des fonctionnalités avec six mois d'avance sur tous les autres. Dans le monde de l'informatique, cet avantage de six mois est fondamental.

Celui qui fait l'OS, par la force des choses, choisit également par exemple la langue dans laquelle la documentation d'utilisation du système d'exploitation est écrite. Que ce soit clair, aujourd'hui, pour les jeunes Français, l'anglais est du chinois donc ils sont forcément pénalisés en faisant face à deux problèmes différents, l'informatique et la langue, deux pédagogies différentes, deux temps différents. Disposer d'une documentation en français pour apprendre à coder permettrait d'être beaucoup plus productif dans les entreprises et, par effet différentiel, d'autres le seraient moins. Il faut jouer collectif, travailler ensemble comme le font très bien les Allemands et les Américains. Ce n'est pas le cas en France.

J'ajoute que des économistes disent souvent à la radio que, à chaque bouleversement technologique, il y a toujours des gagnants et des perdants mais que, cette fois, nous n'avons pas vu les gagnants. Ils sont étonnés que la croissance soit absente. En fait, ils ne regardent pas bien. Aux États-Unis, la filière informatique représente 1 000 milliards de dollars de chiffre d'affaires et un million d'emplois directs.

La marge financière des entreprises françaises est aujourd'hui siphonnée par les coûts des solutions informatiques étrangères. Ce sont des coûts totalement prohibitifs et non justifiés. Nous sommes dans un piège et il est nécessaire de retourner la situation tout de suite. Les systèmes informatiques sont beaucoup trop sensibles et font courir un risque systémique grave à toutes nos entreprises et à notre société.

Il est urgent de changer d'objectif, de passer d'un objectif de toujours plus à un objectif de résilience de nos systèmes. Il est donc nécessaire de disposer d'un *hardware* et d'un OS conçus pour défendre nos intérêts économiques, respecter nos valeurs européennes, notre vision de l'avenir, notre indépendance, en bref, notre souveraineté.

M. le président Jean-Luc Warsmann. Avez-vous une idée du montant d'investissements que représente le développement de ce *hardware* et de cet OS français ou européens ?

M. Denis Psomiades. Nous avons créé un OS et un *hardware*. Ce *hardware* est également 100 % CLESSE. Nous l'avons mis sur le marché et vendu à deux entreprises de la région lyonnaise. Cet OS existe et nous ne demandons aucun financement pour le faire. Nous demandons seulement l'aide des pouvoirs publics, par exemple en aidant cette entreprise qui travaille sur la dissuasion nucléaire française à accepter les systèmes souverains que nous proposons déjà.

M. le président Jean-Luc Warsmann. Vous nous avez décrit la position de l'ANSSI. Cette position vous a-t-elle été communiquée par écrit ? Existe-t-il un mode opératoire de l'ANSSI qui exige qu'une solution dégage un certain montant de chiffre d'affaires pour être agréée ?

M. Denis Psomiades. C'est la réponse qui nous a été faite plusieurs fois.

M. le président Jean-Luc Warsmann. A-t-elle été faite par écrit ?

M. Denis Psomiades. Non, pas par écrit, c'est l'expérience des différents appels à idées ou appels d'offres qui ont eu lieu récemment et d'une communication téléphonique très récente.

M. le président Jean-Luc Warsmann. Souhaitez-vous évoquer un autre sujet ?

M. Denis Psomiades. Je reprends rapidement les questions qui avaient été posées au début de l'audition.

En ce qui concerne notre actualité pour 2021, le déploiement des solutions Business Computer dépend aujourd'hui des pouvoirs publics. Sans leur aide, nous retrouverons le syndrome du DSI.

La crise de la covid-19 nous a impacté car l'année est marquée par des annulations de commandes ou de marchés, notamment dans l'aéronautique.

S'agissant de la façon dont les acteurs publics peuvent concourir à l'émergence de la souveraineté numérique, il faut redéfinir la doctrine en matière de cybersécurité et régler le problème à la source. Il faut aussi jouer collectif, ce qui n'est pas le cas en France.

La question de savoir si la commande publique est suffisamment orientée vers des solutions technologiques françaises est très complexe. Cette réponse nécessite des nuances et il m'est difficile de répondre rapidement.

Le plan de soutien aux entreprises technologiques est actuellement inaccessible pour les petites structures. Les objectifs sont souvent peu pertinents. Dans le cas de la 5G par exemple, l'intérêt stratégique de la développer est douteux et, dans tous les cas, il ne faut la développer qu'à condition qu'elle soit française. Le monde a changé et nous ne travaillons plus avec les deux autres continents. Il est nécessaire que nous défendions nos propres intérêts.

Dans le cas du secteur spatial, qui se fait actuellement dépasser très clairement par les Américains, les choix effectués ont été mauvais et le sont toujours. Je connais d'assez près ce secteur puisque nous avons eu l'occasion d'y travailler.

Sur l'approvisionnement en composants critiques, il serait effectivement intéressant de regarder de près les réseaux de portes programmables *in situ* (FPGA, *Field-Programmable Gate Array*). Un financement a déjà été mis en œuvre et porte ses fruits. Il faut penser aussi aux mémoires, aux technologies de gravure à pas fin que STMicroelectronics a abandonnées pour des questions de coûts. Ce sont des usines à quelques milliards. Je pense que, dans le plan européen de 750 milliards d'euros, la mise en œuvre d'une usine de gravure de composants à pas fin serait un bon investissement. Nous ne sommes plus capables de le faire en Europe depuis longtemps. Pourtant, cela me paraît fondamental pour avoir des composants, notamment des microprocesseurs, performants et efficaces à l'avenir.

En ce qui concerne l'approvisionnement de CLESSE, nous sommes sous le coup d'un possible veto des Américains sur certains composants du fait des *International Traffic in Arms Regulations* (ITAR), ce qui n'est pas acceptable pour les entreprises. Vous pouvez acheter aujourd'hui un composant qui deviendra ITAR demain ce qui fait que vous ne pourrez plus l'exporter. Ces contraintes sont insupportables et il faut que tous ces composants soient fabriqués en Europe pour ne pas avoir à subir des contraintes ITAR.

Il existe aussi des restrictions d'exportation liées à l'utilisation de nouveaux formats de protocoles qui ont été créés aux États-Unis et nous font arriver en retard sur certains marchés alors que nous sommes tout à fait capables de créer nos propres protocoles et nos propres composants.

M. le président Jean-Luc Warsmann. Pourriez-vous décrire plus précisément en quoi nous ne jouons pas assez collectif en France ?

M. Denis Psomiades. Lorsque nous nous adressons au DSI d'une grande entreprise française comme Saint-Gobain par exemple, il faudrait qu'il soit au moins capable de nous ouvrir la porte de la discussion. Pour qu'il le fasse, compte tenu de l'appréhension à laquelle nous nous heurtons sur les systèmes français, il faudrait que la composante publique soit présente, qu'elle donne caution d'une manière ou d'une autre, pas financièrement mais simplement en encourageant ce DSI à utiliser une solution souveraine française existante pour qu'il ne se sente pas coupable de le faire. Ce n'est même pas une question d'argent ; il s'agit de se mettre autour de la table et d'en discuter.

De plus, l'ANSSI dit ouvertement – ce sont des écrits qui se trouvent sur internet – ne pas encourager le fait de choisir une solution souveraine. Le directeur général de l'ANSSI l'a dit dans un discours en 2016 et une communication téléphonique récente me confirme que la doctrine est toujours la même.

Il faut donc d'un côté enlever les freins et de l'autre mettre les gens autour de la table pour créer un collectif ou un groupement d'intérêts économiques qui permette aux DSI, sans prendre le risque de perdre leurs postes, d'accepter des solutions françaises. Le cas de la

dissuasion nucléaire est symptomatique. Il est évident que cela devrait se faire et nous avons pourtant ce blocage.

M. le président Jean-Luc Warsmann. Je vous remercie pour ces avis dont nous tirerons profit au maximum, pour votre liberté de ton et pour les éléments très concrets que vous avez apportés. Je vous souhaite beaucoup de succès et, si la mission peut vous aider à lever quelques blocages, nous essaierons de le faire.

Audition, ouverte à la presse, réunissant des représentants d'entreprises, avec M. Yoann Kassianides, délégué général de l'ACN, Mme Louise Bautista, représentant M. Mathieu Isaia, directeur général de TheGreenBow, M. Arthur Bataille, président de Silicom, fondateur de Seela, M. Jacques de La Rivière, président et cofondateur de Gatewatcher, et M. Sébastien Garnault, fondateur de la CyberTaskForce et de Paris Cyber Week, président de Garnault & Associés

(14 janvier 2021)

Présidence de M. Jean-Luc Warsmann, Président.

M. le président Jean-Luc Warsmann. Avant toute chose, j'exprime mes meilleurs vœux à chacune et chacun, au terme d'une année 2020 des plus difficiles.

Nous reprenons les travaux de notre mission d'information par deux tables rondes. Elles se consacrent à la souveraineté numérique et à la commande publique. En échangeant avec des acteurs publics et privés, notre objectif consiste à voir comment la commande publique peut être mise au service, d'une part de la transformation numérique de nos administrations, d'autre part de la construction d'une forme de souveraineté numérique nationale ou européenne.

Pour la première table ronde, sont présents par visioconférence M. Yoann Kassianides, délégué général de l'ACN, Mme Louise Bautista, représentant M. Mathieu Isaia, directeur général de TheGreenBow qui ne peut participer aux échanges de ce jour, M. Arthur Bataille, président de Silicom, fondateur de Seela, et M. Jacques de La Rivière, président et cofondateur de Gatewatcher. M. Sébastien Garnault, fondateur de la CyberTaskForce et de Paris Cyber Week, président de Garnault & Associés, assiste également à la réunion.

Je les remercie des réponses écrites qu'ils nous ont d'ores et déjà adressées ou pour celles qu'ils nous feront encore parvenir.

M. Philippe Latombe, rapporteur. Je m'associe aux vœux du président pour l'année 2021. J'espère que nous sortirons rapidement de l'état de crise sanitaire et que la mission d'information sera en mesure de reprendre ses travaux autrement qu'à distance.

À titre d'introduction de la présente table ronde, je souhaite en interroger les participants sur plusieurs sujets.

Pouvez-vous d'abord nous préciser ce que recouvre pour vous la notion de souveraineté numérique ? Elle fait l'objet d'une attention croissante de la part des pouvoirs publics depuis le commencement de la crise sanitaire. En raison de son caractère ouvert, nous en avons entendu plusieurs définitions au cours des différentes auditions que nous avons déjà menées. Certains la rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Le regard que vous portez, en tant qu'acteurs privés, sur ce concept nous intéresse. Vous nous préciserez comment vous pensez qu'il peut se traduire concrètement dans les politiques publiques.

J'aborderai ensuite la commande publique, objet direct de notre table ronde. Il s'agit d'un outil puissant puisqu'il représentait près de 87,5 milliards d'euros en 2019, selon le baromètre de l'Assemblée des communautés de France (AdCF) et de la Banque des territoires. Estimez-vous que la commande publique se tourne assez vers des solutions numériques et technologiques françaises ou européennes ? Certaines de ces solutions étant portées par des

petites ou moyennes entreprises (PME), nous aimerions savoir si les PME, ainsi que les entreprises de taille intermédiaire (ETI), parviennent à accéder suffisamment et facilement à la commande publique. Dans le cas contraire, vous nous indiquerez quelles difficultés elles rencontrent.

Enfin, nous évoquerons avec vous l'enjeu de la numérisation des entreprises, particulièrement prégnant depuis le déclenchement de la crise sanitaire. Nous formulerons ici deux interrogations principales. En premier lieu, comment inciter les entreprises à se numériser davantage, c'est-à-dire à recourir à des outils numériques qui leur permettent d'être plus compétitives ? En second lieu, devant un risque croissant, comment développer une culture de la cyberprotection chez les acteurs privés ? M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a récemment confirmé l'augmentation exceptionnelle du nombre des attaques informatiques en 2020, de même qu'il en a souligné l'inventivité des auteurs.

Je vous cède la parole.

M. Jacques de La Rivière, président et cofondateur de Gatewatcher. Depuis une dizaine d'années, la commande publique relative au numérique constitue en France un sujet récurrent. PME et grands groupes français du numérique accèdent à cette commande par le moyen de centres d'achats généralisés, telle l'Union des groupements d'achats publics (UGAP). La difficulté se révèle essentiellement culturelle. Les acheteurs publics ne donnent pas automatiquement leur préférence aux produits numériques français. À contraintes comparables du point de vue des marchés publics, ceux d'autres pays européens, comme l'Allemagne, choisissent spontanément les produits nationaux, avant que d'envisager le recours à des solutions d'origine étrangère. En France, l'acheteur public s'oriente souvent d'emblée vers l'offre américaine. Elle lui paraît mieux garantir son projet. Il faut changer cette approche.

Des initiatives à l'instar de celle que la direction interministérielle du numérique (DINUM) a engagée en faveur d'un nouveau label, vont en ce sens. Ainsi que vous l'avez rappelé, la commande publique ne manque pas d'importance en raison de son volume. Elle est appelée à se renforcer encore du fait de la crise qui sévit. Vecteur d'innovation, source de développement des produits, elle s'avère essentielle pour les PME.

Quinze ans en arrière, lorsque l'entreprise de commerce en ligne Amazon a lancé son offre de services informatiques via internet, ou *cloud computing*, elle a bénéficié, de la part de ses autorités nationales, pendant les deux premières années, d'une commande publique de 600 millions d'euros. Par comparaison, lors de son lancement en France en 2012, Cloudwatt n'a obtenu que l'attribution d'un seul projet public, celui du réseau national de télécommunication pour la technologie, l'enseignement et la recherche (RENATER), pour un total de 200 millions d'euros d'investissement. Cette offre d'hébergement en ligne française a finalement échoué.

Par ailleurs, le personnel de l'administration française tend souvent à redévelopper par ses propres moyens des produits numériques nationaux déjà existants sur le marché. De la sorte, il concurrence ces mêmes produits. En l'absence de mutualisation, de tels développements engendrent de plus des coûts particulièrement élevés. De nombreux exemples existent.

Mme Louise Bautista, TheGreenBow. Sur le premier point soulevé, celui de la définition de la souveraineté numérique française ou européenne, et à côté d'autres interprétations possibles, je perçois fondamentalement deux approches complémentaires. La

première met en avant l'intelligence économique. Elle permet d'intégrer les grands groupes stratégiques, ainsi que les PME, au cercle de la souveraineté numérique. La seconde se concentre sur le secteur public et la continuité du service public.

Aujourd'hui, l'inquiétude principale a d'abord trait au risque de ne pas être en mesure d'assurer la continuité du service public. Le cas de figure s'en présenterait si des plateformes numériques étrangères décidaient d'interrompre leurs prestations. Il pose la question de notre indépendance politique sur la scène internationale. Pour l'heure, afin d'assurer la continuité du service de l'État, nous sommes dépendants de fournisseurs numériques extérieurs et à tendance monopolistique.

À celui de la continuité du service, la notion d'intelligence économique ajoute des critères relatifs à la création d'emplois et à l'accroissement du pouvoir d'achat au sein de l'État.

La formulation d'une critique négative ne saurait prévaloir uniformément. Sur les aspects d'audit et de certification des produits numériques de sécurité, à l'instigation de l'ANSSI à l'échelle nationale et de l'Union européenne à celle du continent, force est de constater une indéniable progression. Les efforts dans le sens d'une homologation des produits permettent d'assumer un début de souveraineté numérique française et européenne.

S'agissant de la commande publique, je reviens, à la suite d'un précédent entretien que nous avons eu, sur l'arsenal juridique existant. Nous disposons de l'instruction générale interministérielle (IGI) n° 1300 et de ses classifications. Dans le respect du droit de la concurrence européen, elle autorise l'apposition d'une mention « Spécial France » lors des appels d'offres inhérents à des commandes publiques.

Les récents échecs relatifs aux commandes publiques de la Banque publique d'investissement (Bpifrance) ou de Health data hub (HDH) montrent combien il fut préjudiciable de n'y pas recourir, particulièrement du point de vue de la protection des données de santé des citoyens. Par comparaison, je doute que, dans ce dernier domaine éminemment stratégique, l'Obamacare (*patient protection and affordable care act*, loi sur la protection des patients et les soins abordables, promulgué en 2010) ait seulement envisagé de recourir à la solution française d'hébergement d'OVHcloud.

Il n'apparaît pas indispensable de légiférer davantage. Utilisons les outils juridiques en vigueur. Au moment des appels d'offres, la mention « Spécial France » implique de ne retenir que des sociétés françaises dans des domaines qui comportent un enjeu de nature stratégique pour la Nation. Ces outils s'appuient sur le travail efficace que les autorités de certification, au premier rang desquelles l'ANSSI en France, assurent depuis plusieurs années.

En revanche, pourquoi ne pas étendre le champ des obligations actuelles en prévoyant celle d'utiliser des produits certifiés pour les identités publiques ou les opérateurs d'importance vitale (OIV) ?

L'adoption du règlement général sur la protection des données (RGPD) a montré le lien entre efficacité des textes et crainte de la sanction pécuniaire. Dès lors, je suggère que nous disposions d'une autorité pleine et entière, avec un budget dédié, qui sanctionne ceux qui ne respecteraient pas les dispositions de cet arsenal juridique que j'évoquais.

M. Yoann Kassianides, délégué général d'ACN. Je souscris aux propos que les deux précédents intervenants ont tenus, tant sur les problèmes qui se posent que sur les avancées que nous relevons.

Organisation professionnelle, l'ACN représente les entreprises de la filière de la confiance numérique en France. La filière de la confiance numérique renvoie notamment à l'identité numérique et à la cybersécurité. Elle se révèle des plus présentes, vivaces et performantes en France. Elle a généré quelque 13 milliards d'euros de chiffre d'affaires en 2019. Elle comprend de nombreuses entreprises, dont des numéros un mondiaux, des ETI, de jeunes et petites entreprises innovantes (*startups*). Elle dispose d'un véritable savoir-faire. Il convient de ne pas l'oublier. L'attention tend à se centrer sur le seul marché du numérique grand public où, de fait, les acteurs français sont moins présents. Ce seul constat ne saurait conduire à tirer la conclusion de leur absence totale du secteur du numérique.

Au sein de l'ACN, une vision large de la notion de souveraineté prévaut. Nous l'entendons d'abord comme le pouvoir suprême reconnu à une nation. Ce pouvoir implique une compétence exclusive sur un territoire donné. À l'évidence, la définition se complexifie en matière numérique. Dans ce domaine en effet, la notion même de territoire apparaît plus difficile à cerner. Une certaine agilité intellectuelle et juridique s'avère nécessaire pour y transcrire le concept traditionnel de souveraineté.

Nous livrant à ce travail, nous aboutissons à assimiler la souveraineté numérique nationale, d'une part, à la capacité pour un État à exercer ses attributions de souveraineté dans l'espace numérique, d'autre part, à sa faculté à utiliser et à protéger contre d'éventuelles attaques des moyens numériques propres qui autorisent cet exercice. En d'autres termes, nous retenons la possibilité pour l'État d'employer des outils numériques au service de ses prérogatives régaliennes.

Quoiqu'étendu, cet ensemble conceptuel demeure opérant. Il permet de regrouper toutes les actions et conclusions utiles à la préservation de la souveraineté nationale.

Pour l'échelle européenne, pertinente de nos jours compte tenu de la concurrence internationale et de la dimension des blocs tant économiques que géostratégiques en présence, nous préférons, à l'ACN, employer l'expression d'« autonomie stratégique ». Celle-ci nous paraît mieux préserver la logique juridique. Nous ne perdons pas de vue que traditionnellement le droit réserve le concept de souveraineté aux seules entités étatiques. L'Union européenne ne revêt pas la qualité d'un État au sens strict. Divers traités internationaux lui ont plutôt délégué une partie des prérogatives de ses États membres.

Comment la notion de souveraineté numérique, ainsi que son pendant d'autonomie stratégique, se traduisent-ils ?

Dès lors qu'il exerce des missions régaliennes de manière numérique, il importe que l'État veille concomitamment à disposer des outils appropriés et à conserver l'exclusivité de sa compétence.

À titre d'exemple, je citerai l'identité et l'état civil. La transposition numérique de l'état civil pose une difficulté. Nous remarquons que de nombreuses identités cohabitent dans le domaine numérique. Parmi elles, les plus pertinentes ne sont pas celles que les États européens contrôlent.

Si l'État entend poursuivre sa mission déterminante d'identification de ses ressortissants, le sujet de l'identité numérique devient central. Des travaux en ce sens se poursuivent. Leur résultat devra se matérialiser à brève échéance, tant les acteurs privés qui, la plupart étrangers, développent leur propre identité numérique, progressent avec célérité. Les outils permettant d'exercer des prérogatives régaliennes sont à considérer prioritairement.

Une autre manière de préserver la souveraineté nationale ou l'autonomie stratégique européenne consiste à s'appuyer sur des acteurs à la fois disponibles et performants.

Il convient de plus que l'État entretienne une vision stratégique. Elle suppose la mise en cohérence de l'ensemble des actions qui relèvent du numérique, au regard de la sécurité, de la confiance et de la souveraineté.

Le numérique reste encore trop diffus. Nous le retrouvons dans toutes les applications et interactions sociales et économiques. Chaque sujet spécifique dispose encore de ses propres développements numériques et d'un traitement local. Un effort de cohérence s'impose. Le numérique, la confiance dans le numérique, constituent des axes d'attention prioritaires. Les affrontements à venir s'effectueront dans le domaine numérique. Pour l'État, prendre l'initiative requiert ici une exigence de transversalité et d'homogénéisation. Une vision de surplomb, un niveau décisionnel adéquat, doivent nous garder de l'actuelle dissémination des décisions, assurément contreproductive.

Dans l'initiative publique, la question de la souveraineté numérique prend toute sa place quel que soit le secteur d'activité considéré. Elle semble d'emblée évidente en matière de défense ou de sécurité nationale. Elle apparaît de prime abord moins nettement dans d'autres domaines de l'action publique mais ne s'y impose pas moins. À notre avis, et peut-être sous forme d'études d'impact, l'attention à la souveraineté mérite de concerner tout processus de décision ayant trait au numérique. En ce sens, nous la rapprocherions des préoccupations d'ordre environnemental, elles-mêmes nécessairement transversales et impliquant une étude préalable des effets des décisions à prendre. Une approche de ce type nous aurait évité bien des désagréments et débats.

En dernier lieu, lorsque l'État se comporte en qualité d'acheteur, il se doit de faire montre d'exemplarité. Il s'agit évidemment qu'il se conforme aux préoccupations de souveraineté numérique, mais encore qu'il s'assure, au-delà de la seule origine nationale du produit acheté, que l'action qu'il mène aide à conforter une filière par nature stratégique puisqu'elle lui apporte les outils à même de maintenir sa souveraineté en conservant la maîtrise de son espace numérique. Outre la prise en compte de la nationalité du produit, l'État s'attachera par exemple à l'existence d'un environnement connu et de confiance, ou simplement à celle d'un approvisionnement interchangeable, sans tension ni contrainte.

Vous l'aurez compris, le message que nous entendons porter devant vous consiste d'abord à ce que la considération de la souveraineté embrasse l'ensemble des initiatives publiques qui comprennent une dimension numérique ; c'est-à-dire vraisemblablement toutes les actions publiques, tant nous imaginons mal que cette dimension en puisse désormais être absente.

M. Arthur Bataille, président de Silicom, fondateur de Seela. La société Silicom est une société de conseil. La société Seela propose, en partenariat avec Airbus, une formation en cyberentraînement. Elle a elle-même fondé un groupement, FIRST (French Industrials for Resilience, Security & Trust), qui promeut les enjeux de sécurité sous l'angle des outils, de la formation et de l'acculturation des entreprises, principalement à destination des ETI et PME.

Je partagerai avec vous les enseignements de mon expérience en tant que dirigeant de PME.

La crise sanitaire nous a permis de nous forger une vision claire de l'état actuel du numérique en France et, en particulier, de son niveau de développement au sein des entreprises françaises. Au cours de cette crise, nous avons été confrontés à une élévation significative des

attaques, tant en nombre qu'en qualité. Elles ont perturbé des entreprises françaises dans leur modèle économique.

À mon sens, la souveraineté numérique concerne également les entreprises françaises, ainsi que les collectivités territoriales. Elle interroge la capacité de résistance de nos entreprises dans leur création de valeur ajoutée, dans leur recherche de développement, dans la défense des actifs dont elles disposent, notamment en matière de propriété intellectuelle.

Nous concentrons généralement notre attention sur les OIV. L'ANSSI surveille de près les risques d'attaques susceptibles de les affecter. L'Agence nationale pour le numérique (ANPN) leur garantit un certain niveau de sécurité. En revanche, nous ne nous préoccupons pas assez des sous-traitants des grands groupes et des administrations. Eux aussi hébergent des données.

Indépendamment de considérations qui prôneraient l'utilisation des seuls produits français ou européens, il convient de relever un problème de maîtrise des techniques numériques. En qualité de dirigeant d'une société de conseil, je m'interroge sur la capacité de la France à former ses jeunes des universités et des écoles d'ingénieurs dans les domaines de la sécurité informatique. Nos formations se focalisent par trop sur des métiers dits généralistes. Elles ne spécialisent pas assez.

Au contraire, les filières de formation par alternance paraissent répondre mieux aux problématiques et enjeux actuels dans ces domaines. En dépit du cursus généraliste que j'ai moi-même suivi, celui des classes préparatoires et des grandes écoles d'ingénieurs, sur le constat de son manque de pragmatisme, j'embauche plus favorablement des alternants. Leur première expérience professionnelle les amène à développer une expertise véritablement technique.

Certes, administrations, ministères et grands groupes entretiennent les moyens de maintenir en toute sécurité la capacité opérationnelle de leurs systèmes d'information. En revanche, à l'occasion de la crise sanitaire, souvent les directeurs des systèmes d'information (DSI) des PME ont dû mettre en place des outils de communication à distance, des réseaux privés virtuels (*virtual private networks*, VPN), sans réellement savoir ni comment les administrer, ni bénéficier d'équipes formées à ces produits.

En matière numérique, la question de la formation continue, particulièrement à l'aide d'organismes tels que les opérateurs de compétences (OPCO), me paraît posée. Je la juge fondamentale. Sauf erreur, je ne pense pas que des appels d'offres aient été publiés ces derniers mois qui viseraient à accompagner les entreprises dans la formation de leurs collaborateurs. Je soutiens que de cette formation dépend en partie la défense de notre souveraineté numérique.

M. Philippe Latombe, rapporteur. Mme Louise Bautista, j'aimerais revenir sur vos propos. Vous avez évoqué les exemples des appels d'offres de Bpifrance et de HDH. La mission d'information consacrera une audition aux données de santé et entendra les représentants de HDH. Elle a d'ores et déjà auditionné ceux de Bpifrance. À la suite de réponses similaires que nous avions précédemment reçues de la part d'autres intervenants, ils nous ont expliqué avoir choisi de recourir à Amazon Web Services (AWS) car cet acteur propose à ce jour la meilleure qualité de service du marché, avec la suite logicielle la plus aboutie. Ils en soulignaient une avance d'une ampleur telle qu'elle semblait exclure toute solution française ou européenne, à l'exception peut-être, moyennant quelque temps, de Gaia-X.

Ce sentiment revêt-il une dimension culturelle, ainsi que, M. Jacques de La Rivière, vous le suggériez ? L'acheteur public préfère-t-il d'emblée, sans autre examen, une solution américaine à une offre française ? Au contraire, existe-t-il entre elles une différence de niveau si marquée que le choix ne peut autrement s'orienter ?

Une autre question s'adresse à M. Arthur Bataille, sur les aspects de formation. Il se dit communément que la filière française ne manque pas de reconnaissance, pour ce qui touche notamment à la cybersécurité, à l'identité et à la confiance numériques. Pourquoi n'obtenons-nous pas une meilleure diffusion dans les entreprises et les administrations des connaissances de nos spécialistes dans ces domaines ? Quel échelon fait-il défaut ?

Mme Louise Bautista. Je dirai après M. Yoann Kassianides qu'imposer en toutes circonstances, dans le choix de produits informatiques, un simple critère de nationalité ne prendrait guère de sens. Nous ne saurions exclure des considérations d'excellence. Poser une obligation de choisir systématiquement une solution française ne favoriserait pas la qualité de l'offre nationale.

En revanche, l'apposition d'une mention « Spécial France » s'avère pertinente dès lors que nous constatons un enjeu crucial pour la Nation, la présence de données qui lui sont stratégiques. Dans ces conditions, le choix du meilleur produit devient secondaire. La considération de l'autonomie stratégique devrait toujours l'emporter sur le poids des argumentaires certes efficaces de commerciaux, par exemple ceux d'Amazon, qui savent mettre en avant auprès des administrations les fonctions et applications évoluées de leurs solutions d'hébergement des données. Le choix se circonscrirait alors aux offres nationales d'OVHcloud et d'Outscale. Quoique moins étendues sans doute que celles de leurs principaux concurrents étrangers, elles s'avèrent de qualité et propres à répondre aux besoins auxquelles nous les destinerions.

Je ne porte aucune accusation à l'encontre de Bpifrance. Des faiblesses, des pressions et des discours commerciaux interfèrent dans la prise des décisions. En pareille occurrence, j'estime néanmoins que le choix de recourir à une plateforme étrangère ne devrait pas être ouvert. Il appartient au législateur d'intervenir. Amazon est une entreprise américaine. La France est membre de l'OTAN et évidemment l'alliée des États-Unis. Les deux États n'en sont pas moins des concurrents. Concevrions-nous de nous adresser à la Corée du Nord ou à la Chine, afin de bénéficier de leurs solutions numériques ? Nous ne leur confierions certainement pas les données de nos entreprises les plus prometteuses dans le domaine des techniques de pointe, les « licornes » de demain. Pourquoi y consentir avec une société américaine ? Je doute qu'une entreprise telle qu'Airbus, fort bien consciente des enjeux de l'intelligence économique, accepterait de seulement l'envisager.

M. Philippe Latombe, rapporteur. Quand nous interrogeons Bpifrance ou d'autres acteurs, nous en recevons une réponse qui tend à amoindrir la portée du risque au motif que les données demeurent continûment chiffrées et que la clé de chiffrement leur appartient en propre. En aucun cas, nous disent-ils, l'hébergeur, qu'il s'agisse d'Amazon, de Microsoft Azure ou de n'importe quel autre, n'en dispose. Dans le cas précis de Bpifrance, l'autorité de certification compétente, l'ANSSI, a validé le choix de recourir à AWS. De nouveau, je m'interroge sur la possibilité d'un problème d'ordre principalement culturel.

M. Arthur Bataille. M. le rapporteur, vous avez précédemment utilisé le terme de « diffusion ». Je défends avec ferveur la qualité de notre industrie et de nos ingénieurs français. Néanmoins, en matière numérique, nous nous confrontons à une évolution extrêmement rapide des techniques à l'œuvre. Elle s'accélère sans cesse, au service d'un monde lui-même en perpétuel changement. Les principes, les procédures et les moyens de la sécurité des systèmes

d'information qui étaient valables trois ans plus tôt sont déjà révolus. La problématique de la sécurité informatique n'est pas récente. La première attaque sur un réseau en ligne remonte à 1989.

Notre difficulté consiste donc à adapter rapidement nos programmes pédagogiques à la réalité, aux outils et aux enjeux. Je réitère que la formation en alternance présente ici un avantage certain. S'effectuant en entreprise, elle imprègne les étudiants de cette réalité, de ces outils et enjeux actuels.

Par ailleurs, je ferai état du danger de la précipitation de la commande publique. La nécessité de bénéficier d'une solution à brève échéance conduit à pencher vers la solution la plus aisément accessible. Vous avez mentionné la question du chiffrement des données. Ses enjeux s'avèrent complexes et souvent peu maîtrisés techniquement. Thomas Baignères, fondateur et président de l'entreprise Olvid, pourrait en témoigner. La clé de chiffrement n'offre pas une sécurité absolue. La détenir en exclusivité ne donne pas l'assurance d'une parfaite sécurisation des données et de leur inaccessibilité par un tiers.

Je partagerai avec vous une anecdote personnelle. L'un des responsables informatiques de l'entreprise que je dirige, qui en a élaboré tout le réseau intermédiaire, a pu un temps penser que l'intégralité de nos données étaient cryptées du fait qu'elles ne circulaient que selon un mode binaire, en interne entre nos différents sites.

Dans les débats qui nous animent, le constat reste le même, quoique à une échelle bien supérieure. Les techniques actuelles ont pris une envergure telle que nous n'en maîtrisons la portée ni la façon dont elles sont utilisées.

Mme Louise Bautista. Au sujet des clés de chiffrement, au centre de la réponse de Bpifrance, je renverrai à une autre audition que votre mission d'information parlementaire a organisée et dont j'ai pris connaissance. Il s'agit de celle de M. Charles Thibout, tenue le 12 novembre 2020. S'appuyant sur un rapport d'experts militaires mandatés par le ministère de la défense en 2008, au moment d'évaluer un projet que Microsoft avait présenté, votre interlocuteur commençait par rappeler que nos services de sécurité nationaux avaient alors établi que la pratique dite des « portes dérobées » (ou *backdoors*) dans les logiciels qui portent sur des données stratégiques, et quand bien même ils émanent d'alliés, était courante. Rien ne garantit jamais contre le risque de cette pratique, même la possession en propre de clés de chiffrement. Celle-ci n'assure aucunement de l'intégrité et de la stricte confidentialité des services.

Un second risque a trait à la maintenance de l'hébergement des données numériques et à la continuité du service public. Un différend toujours possible, y compris avec un allié – tel celui qui émergea au début des années 2000 entre la France et les États-Unis au sujet du veto que la première menaça d'opposer contre une nouvelle guerre en Irak –, pourrait amener le fournisseur à interrompre sa prestation. Parmi d'autres, une réponse de cette nature revêtirait la forme d'une arme diplomatique. Ses conséquences ne seraient pas anodines. L'hypothèse n'en est certainement pas à considérer avec légèreté.

M. Jacques de La Rivière. Dans le domaine du numérique, la France compte des acteurs de premier plan sur la scène internationale, des « champions ». Je pense par exemple à Atos, Capgemini ou Sopra Steria. Cependant, ils ne proposent qu'une offre de services. Nous avons par ailleurs échoué s'agissant des produits.

La raison en tient au marché local. Sous l'effet d'un cercle vicieux, ce marché commandant essentiellement des produits américains, ainsi qu'en témoigne le choix de

Bpifrance, au moment de la mise en place des prêts garantis par l'État (PGE), de s'adresser à Amazon, les offreurs français ou européens n'y disposent pas d'un volume de commandes suffisant pour exister face à la concurrence étrangère et proposer un niveau de fonctionnalités équivalent.

Au contraire, en matière de prestation de services informatiques, outre un vrai soutien à l'export, les acteurs français bénéficient notamment des spécificités du droit du travail national. Ne souhaitant pas embaucher directement et rester en mesure de changer de ressources, les donneurs d'ordre leur font prioritairement appel.

S'agissant des produits informatiques, aucune dynamique réglementaire n'intervient. Seules sont à relever d'occasionnelles prescriptions que l'ANSSI émet sur la robustesse des produits. Certaines ont par exemple pu intéresser les sondes de détection des OIV que Gatewatcher élabore. Néanmoins, en l'absence d'obligations réglementaires systématiques sur la certification des produits, à même d'en garantir la robustesse et par suite de répondre aux exigences de la souveraineté, nous resterons confrontés à l'offre massive de produits étrangers.

Pour mon entreprise, j'ai bénéficié d'un PGE. À cette occasion, j'ai constaté la simplicité d'utilisation de l'application informatique qui se rapporte au dispositif. Les champs à remplir tiennent en une unique page en ligne. N'importe quel hébergeur pouvait prendre en charge cette application et les données qu'elle génère, avec ou sans clé de chiffrement. OVHcloud, Outscale, ainsi que la multitude des hébergeurs indépendants qui existent en France et en Europe, en avaient la capacité. Néanmoins, pour des raisons de facilité, parce qu'ils sont d'abord formés sur des produits américains, les développeurs de l'application des PGE de Bpifrance ont choisi de s'orienter, sans autre interrogation, vers ce qu'ils connaissaient le mieux, l'offre d'AWH.

Mme Louise Bautista. Je partage sans réserve ce qui vient d'être dit. Nous comptons en effet en France des champions du numérique. Nous ne le devons cependant pas uniquement à nos talents. Historiquement, le plan gouvernemental Calcul que le président Charles de Gaulle a lancé en 1966, avec les financements d'entreprises qu'il emportait, y a également fortement contribué. Il a permis le développement d'entreprises telles qu'Atos, Bull, France Télécom, devenue Orange, Capgemini, ainsi qu'une myriade de PME, dont TheGreenBow pour laquelle je travaille. Une initiative, une impulsion politique majeure a rendu possible ces réalisations.

Désormais, un ministère du numérique, un arsenal juridique renforcé et des mesures concrètes seraient nécessaires. Au-delà des paroles, nous attendons des acteurs politiques qu'ils favorisent un nouvel et indispensable élan. À tous les niveaux, les compétences existent. Nous avons évoqué les produits de sécurité. Dans ce domaine, TheGreenBow réalise du chiffrement depuis vingt-deux ans, y compris pour des sociétés américaines. Les exemples de réussites et de reconnaissance mondiale sont nombreux. Nous disposons de belles entreprises, de startups innovantes, d'excellentes écoles. Il ne saurait être question d'entretenir un quelconque complexe d'infériorité. Seule une impulsion nous manque.

M. Philippe Latombe, rapporteur. Selon vous, comment procéder ? Doit-il s'agir d'une initiative strictement française, avec un ministère dédié et un plan spécifique, ou l'échelon européen vous semble-t-il mieux approprié ?

Mme Louise Bautista. Les deux niveaux français et européen doivent se combiner. Certes, nous ne saurions rien entreprendre sans l'Europe, notamment en matière de certification. En revanche, pour certains projets, notamment ceux qui touchent à l'intelligence économique, dans des domaines où nous pourrions avoir des concurrents européens, sur des

sujets qui mettent en cause la continuité de l'État, une souveraineté numérique française demeure incontournable. Elle se traduit par exemple par la mention « Spécial France ».

Trop attendre de l'Europe constituerait un écueil. En dépit de l'énergie que déploie le commissaire européen au marché intérieur, M. Thierry Breton, il nous faut également promouvoir le changement à l'échelle nationale. L'un ne va pas sans l'autre.

M. Arthur Bataille. Si un ministère du numérique se forme, il importe qu'il ne limite pas son intervention aux aspects réglementaires et au RGPD. La problématique dont nous traitons revêt une dimension essentiellement technique.

J'apprécierais que des groupes de travail ministériels évaluent l'état précis de la situation. Nous devons également renforcer les moyens de l'ANSSI. Il s'agit d'accompagner les entreprises françaises dans la préservation de la sécurité de leurs infrastructures et de poursuivre la mise en place de procédures de sécurité à l'usage des collectivités territoriales.

À l'échelle de l'Union européenne, le partage des connaissances et des compétences apparaît par ailleurs déterminant si nous entendons aboutir à l'élaboration d'une structure souveraine de *cloud*. La crise sanitaire porte aujourd'hui un coup d'arrêt fâcheux au programme d'échange des universités européennes. Il est fondamental qu'il puisse reprendre à brève échéance.

En tout état de cause, les principaux acteurs de l'industrie ou de la banque françaises déploient leurs ramifications dans le monde entier. Les considérations tenant au numérique ne sauraient se restreindre au seul territoire national.

Enfin, du point de vue de notre souveraineté, je soulignerai l'importance des plans d'actions qui s'appuient sur le crédit d'impôt recherche. Je remercie les pouvoirs publics de continuer à financer ainsi la recherche française, en réservant les aides accordées aux entreprises nationales.

M. Yoann Kassianides. Je souscris à l'idée selon laquelle il convient de mêler les deux niveaux français et européen.

La question de la souveraineté numérique se pose avec acuité du fait de l'omniprésence de produits d'origine américaine ou asiatique. La crise sanitaire a mis en lumière notre dépendance à ces produits. Elle a aussi provoqué une prise de conscience générale. Chacun mesure désormais la nécessité d'assurer notre souveraineté par nos propres moyens.

Devant les blocs majeurs qui se sont constitués, la menace apparaît d'un ordre géopolitique et géostratégique. La réponse ne peut être strictement française. L'échelle pertinente est celle de l'Europe.

Pour autant, il ne s'agit nullement de dénier toute possibilité d'initiative nationale. Du fait de l'excellence de ses entreprises, de sa recherche, de son expérience dans le domaine de la sécurité numérique, la France conserve des atouts de taille. Rappelons que l'invention de la carte à puce lui revient. Elle possède des compétences reconnues mondialement en matière de sécurisation et de chiffrement. Il nous appartient de nous appuyer sur ces atouts et de les porter au niveau européen.

Un tel niveau s'avère cohérent. Les membres de l'Union européenne partagent un même système de valeurs. Nous ne l'affirmerions pas s'agissant de la Chine, ni même des États-Unis. La première fonction des outils de confiance numérique vise à nous permettre de

déployer nos activités dématérialisées conformément à notre système de valeurs. Ils sont les garants de ces valeurs quand il s'agit de le transposer dans le monde numérique.

De plus, la pertinence de l'échelle européenne se révèle sous l'angle économique. Revenons à la question de la certification. À ce jour, au sein de l'Union européenne, vendre un produit soumis à des obligations de certification impose encore de s'adresser, tour à tour, à chacune des autorités nationales de certification compétentes. Cette contrainte entraîne une complexité et des coûts supplémentaires non négligeables. En comparaison de la situation de leurs principaux concurrents internationaux, elle constitue un frein au développement économique des acteurs européens.

L'Union européenne s'attache à lever de telles barrières. En 2019, le *cybersecurity act* a ouvert la voie de certifications valables dans l'ensemble de l'Union. Nécessairement long, le processus de discussion se poursuit autour de critères communs. Il contribuera à définir un espace économique et numérique européen comparable aux blocs concurrents dont nous faisions état. Il se révèle primordial pour les entreprises européennes qui développent des produits numériques. Elles doivent pouvoir s'appuyer sur un marché domestique équivalent à ceux de leurs concurrents les plus actifs.

Enfin, des prérogatives régaliennes demeurent l'apanage des États. Elles ne relèvent pas de la compétence de l'Union européenne. Elles maintiennent l'utilité d'une souveraineté numérique nationale.

La combinaison des deux échelons, ceux de l'État et de l'Union, doivent s'harmoniser intelligemment. Assurément, la France se trouve en position de jouer un rôle de « pilote ». Sa filière numérique et son autorité de certification, l'ANSSI, jouissent de la reconnaissance de ses partenaires européens. Elles ont vocation à servir d'exemple. Il faut les y encourager. Les entreprises françaises en tireraient un avantage certain dans la conquête du marché numérique européen, s'il se concrétise.

Il revient donc à l'État d'élaborer une vision unifiée et de faire montre de la volonté d'obtenir un socle national fort, pour le porter à l'échelle de l'Europe, à même ensuite d'en assurer une diffusion plus large.

M. Philippe Latombe, rapporteur. Sans intention polémique, j'aimerais connaître le regard que vous portez sur la DINUM et sur son rôle. Sa création entendait précisément harmoniser l'action de l'État dans le domaine du numérique. Jugez-vous que la DINUM influence efficacement la commande publique qui s'y rapporte ?

M. Jacques de La Rivière. Au sein de la DINUM, la mission Label élabore actuellement un label destiné à la commande publique française. Il orientera les décideurs vers l'achat de solutions nationales ou européennes. Même tardive, l'initiative en paraît bonne. Elle contribuera au changement progressif de la culture de l'achat public qui, pour l'heure, se tourne prioritairement vers des offres étrangères.

Mme Louise Bautista. J'estime que l'élaboration d'un label appelé à éclairer les commandes publiques constitue une excellente nouvelle. Elle marque une évolution nette par rapport à ce qui a prévalu quelques années auparavant. Je pense notamment au recours à l'application Tchap, de conception britannique, quand des *startups* nationales, telles qu'Olvid, offraient des solutions au moins équivalentes, avec une qualité de chiffrement irréprochable.

Par ailleurs, bien que TheGreenBow s'emploie à sécuriser les connexions de télétravail des agents du secteur public et assure, par conséquent, une mission des plus stratégiques

actuellement, j'ai peu eu affaire à la DINUM. Il m'a fallu m'adresser à chacun des ministères concernés.

M. Philippe Latombe, rapporteur. Au nom de TheGreenBow, vous avez donc entretenu des relations ministère par ministère ? Nous expliquez-vous qu'aucune réflexion globale ne s'est engagée sous l'impulsion de la DINUM ?

Mme Louise Bautista. Je vous le confirme. Néanmoins, nous n'avons pas essuyé de fin de non-recevoir auprès de la DINUM. Simplement, lorsque le premier confinement a commencé, différents ministères nous ont joints et nous en avons appelé d'autres. Nous avons lancé une opération intitulée « le VPN français ». Nous proposions une offre à un tarif préférentiel aux collectivités territoriales ainsi qu'aux établissements publics. Nombreux sont ceux qui nous ont sollicités, sans que la DINUM n'intervienne. Cependant, l'opération s'effectue depuis lors dans des conditions tout à fait satisfaisantes.

M. Yoann Kassianides. Nous mettons ici le doigt sur une difficulté centrale du sujet de la confiance numérique. La propension de chaque « verticale », qu'il s'agisse des ministères ou des secteurs d'activité, consiste à traiter en interne les questions qui l'intéressent, en l'occurrence celle de la numérisation.

Introduire une part de transversalité, qu'elle soit interministérielle au niveau national, interétatique au plan européen, ou encore intersectorielle, s'avère assurément complexe à réaliser. Une solution homogène, applicable uniformément, relève de la gageure. Tout secteur, tout domaine, chaque verticale, comprend des spécificités. Nous ne pouvons les ignorer. Je laisse de côté les questions de chapelles et de prérogatives que chaque verticale aura tendance à défendre pour les conserver. Les sujets stratégiques imposent de les dépasser.

Il faut tendre à une certaine proportion de transversalité et chercher, du moins, à l'accroître. Sont positives les initiatives qui, d'une manière ou d'une autre, y contribuent. Celles de la DINUM comptent parmi leur nombre. L'équilibre reste à trouver entre transversalité, effort d'homogénéisation, d'une part, et personnalisation nécessaire à chacune des verticales, d'autre part.

Pour l'heure, nous constatons que l'ensemble des questions de sécurité et de confiance numériques se traitent d'une façon verticale.

Mme Louise Bautista. Si mon entreprise n'a pas entretenu de relations avec la DINUM, je tiens en revanche à souligner une initiative du secrétariat d'État chargé du numérique. Au commencement du confinement, ce secrétariat d'État a mis en place une page internet comportant la liste des entreprises françaises du numérique – *startups*, PME, grands groupes – qui souhaitaient répondre par des offres de solidarité à la numérisation contrainte de l'économie. La page répertoriait l'opération de TheGreenBow, « le VPN français », et lui a permis, ainsi qu'à d'autres acteurs, de distribuer gratuitement un nombre élevé de licences.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder d'autres aspects ?

M. Arthur Bataille. Je soulèverai cinq points qui me semblent mériter l'attention de la représentation nationale.

Il s'agit d'abord d'aider et de subventionner universités et écoles en France, afin qu'elles aillent plus avant dans leur démarche pédagogique. Nos établissements d'enseignement doivent disposer de moyens et outils à la mesure des enjeux. Ils souffrent durement de la crise sanitaire qui impose l'éloignement de leurs étudiants.

Nous suggérons ensuite d'augmenter le montant des budgets alloués à la formation dans les entreprises. Une politique résolue doit inciter les entreprises à former leurs collaborateurs.

De plus, nous encourageons la création d'un groupe de travail sur les enjeux de souveraineté numérique et les technologies à valoriser en France, voire en Europe. Il réunirait opportunément les experts de la direction générale de l'armement (DGA) du ministère des armées et ceux de l'ANSSI.

M. Philippe Latombe, rapporteur. En somme, vous évoquez la création d'un équivalent de la *defence advanced research projects agency* (DARPA), l'agence du département de la défense des États-Unis.

M. Arthur Bataille. Nous disposons en France de compétences précieuses au sein de différents ministères sur les aspects techniques des métiers du numérique.

J'ajoute la nécessité de subventionner la recherche, de même à la hauteur des enjeux que nous nous fixons. Je regrette que nous déterminions aujourd'hui les subventions à l'aune de la création de valeur ajoutée par les entreprises et non en fonction du coût réel que la recherche représente pour elles.

Enfin, nous appelons de nos vœux la mise en place d'un plan européen en vue de la conception d'une plateforme en ligne qui exposerait l'offre disponible de produits numériques européens.

M. Philippe Latombe, rapporteur. Je prends note de vos cinq propositions.

Mme Louise Bautista. Je souhaite à mon tour vous en soumettre cinq autres.

Générale, la première invite à passer des paroles aux actes. Nous entendons de nombreux propos fort intéressants. Il s'agirait de les mettre, au moins pour une partie d'entre eux, en pratique. La présente table ronde se déroule par visioconférence. Je note qu'il nous faut à cette occasion utiliser l'application Zoom, une application américaine. Or, utiliser un outil de visioconférence souverain ne relève pas de l'impossible, ni seulement du très difficile. En France, des entreprises certifiées par l'ANSSI, comme Tixeo ou Private Discuss du groupe lyonnais PIMAN, le permettent sans rien céder sur la qualité du service.

La deuxième reprend l'une des premières idées que j'ai précédemment présentées. Elle concerne la création d'une instance de contrôle. Celle-ci aurait pour fonction de faire respecter, sous peine d'amende, l'obligation de certification des produits, ainsi que l'application de la mention « Spécial France » lors des appels d'offres. La proposition suppose de légiférer. La perception du montant des amendes serait susceptible de compenser la dépense liée au budget à consacrer à la nouvelle structure.

La troisième proposition revêt un caractère social. Lorsque j'observais que nous disposons en France des compétences utiles en matière de cybersécurité, j'omettais de signaler qu'elles n'offrent pas exactement l'image d'un modèle de mixité. De fait, les femmes ne représentent qu'environ 11 % de l'effectif total de la filière en France. À un stade décisif, nous nous passons fâcheusement d'un réservoir de talents supplémentaires. Certains pays asiatiques ou Israël ont lancé de vastes initiatives destinées à attirer un nombre plus élevé de femmes vers les métiers de la sécurité. Nous serions bien inspirés de les imiter dans cette voie.

Une quatrième proposition a trait à la sensibilisation à la cybersécurité et aux enjeux d'autonomie stratégique ou de souveraineté numérique, non seulement des établissements d'enseignement supérieur et des professionnels, mais encore des élus, aussi bien locaux que nationaux. Constatant que Google a engagé des initiatives en ce sens à l'attention des PME, je précise plaider en faveur d'une sensibilisation par un ou plusieurs opérateurs français.

Enfin, à la suite d'une tribune publiée à ce sujet, la cinquième proposition que je porte défend la création d'un ministère du numérique. Elle semble recueillir le consensus des acteurs français du secteur. Ni un secrétariat d'État ni une direction interministérielle ne suffisent. À l'approche de la présidence française de l'Union européenne, se doter d'un ministère de plein exercice prendrait de plus valeur d'exemple.

M. Philippe Latombe, rapporteur. Je partage vos réserves au sujet de l'application Zoom. Je suis le premier à en regretter l'utilisation pour nos auditions et tables rondes. Nous incitons autant que nous le pouvons le service informatique de l'Assemblée nationale à changer rapidement d'outil.

M. Jacques de La Rivière. Je me permets de signaler que la *startup* française Livestorm propose également une solution de remplacement à Zoom. D'un emploi des plus simples, elle fonctionne de manière parfaitement satisfaisante. Elle permet à l'utilisateur de créer lui-même ses liens de connexion pour des réunions à distance de type conférence téléphonique ou conférence en ligne (webinaire), sans passer par son service informatique. Si vous le souhaitez, nous nous tenons à votre disposition pour vous accompagner dans le choix d'une nouvelle application.

S'agissant des mesures à vous suggérer, je me concentrerai sur la commande publique. Essentielle, elle s'avère en l'état un obstacle au développement de solutions numériques françaises, en particulier dans le domaine de la cybersécurité.

La mise en place d'une certification obligatoire pour les produits achetés en Europe est essentielle. Les raisons en tiennent non seulement aux contraintes du marché local, afin de permettre aux industries européennes de mieux s'exporter, mais aussi à la robustesse même des produits. La récente attaque informatique qui a affecté Microsoft et FireEye en touchant l'un de leurs fournisseurs en supervision, SolarWinds, a montré les conséquences de l'absence de toute exigence de robustesse et de résistance à l'égard de logiciels. En l'occurrence, elle a offert une voie d'entrée béante chez Microsoft, FireEye et les quelque 18 000 autres clients de SolarWinds.

Lors de l'achat d'un véhicule, il semble évident à tout un chacun que les ceintures de sécurité ou le système antiblocage des roues (ABS) fassent l'objet de certifications précises. Il nous faut adopter une attitude semblable au moment d'acquérir un logiciel. Je dirai que nous manquons encore de maturité devant les produits numériques. Le temps viendra où nous porterons comme il se doit toute notre attention à la certification de leur robustesse.

M. Yoann Kassianides. Pour ma part, j'insisterai sur l'importance de bien concevoir, notamment au sein de la représentation nationale, que notre secteur de la confiance numérique se compose d'entreprises de pointe, c'est-à-dire d'entreprises performantes.

Au regard de la commande publique, je préconise avant tout achat effectif de s'enquérir de ses effets du point de vue de la souveraineté. J'abonde dans le sens des propos qui viennent d'être tenus au sujet de la certification. Elle se révèle décisive à double titre.

D'une part, elle permet de vérifier que le service proposé par l'État n'emporte pas de problématique majeure de souveraineté. En substance, il s'agit de s'assurer de la maîtrise des données, de leur stockage d'une manière bien définie et sans possibilité qu'elles servent à d'autres fins que celles attendues.

D'autre part, une certification rigoureuse, au sens où l'entendent l'ANSSI ou l'agence européenne chargée de la sécurité des réseaux et de l'information (*european network and information security agency*, ENISA), garantit la protection du service, ou cybersécurité. Ainsi que le remarquait l'intervenant précédent, elle donne également à nos entreprises, du fait de leur excellence dans ce registre, un avantage certain. Leurs concurrents internationaux s'appuient d'abord sur leur force financière et leur capacité en matière de marketing.

L'exigence de robustesse des produits numériques devrait donc occuper une place centrale. La crise sanitaire actuelle nous en donne une occasion historique.

La demande de numérisation connaît un essor sans précédent. La pandémie a contraint des millions de personnes à recourir au télétravail quand nul n'y était vraiment préparé. Les entreprises ont compris l'importance de la numérisation de leurs activités.

La cybersécurité et la confiance numérique se construisent dès le départ du projet de numérisation ; la souveraineté numérique doit être prise en compte en amont de la commande publique. Il convient des les y intégrer d'emblée au risque de n'y parvenir que beaucoup plus difficilement, voire plus du tout, ultérieurement.

Les enjeux de la souveraineté numérique sont d'ordre stratégique. Ils priment toute autre considération lors de l'acquisition d'un produit informatique. Il importe de définir cette souveraineté comme une priorité nationale, en ne perdant pas de vue qu'elle s'inscrira nécessairement dans un cadre européen. Bien conçus, les outils numériques servent les valeurs fondamentales qui sont celles de l'Europe. Porteur, ce créneau est susceptible d'entraîner l'ensemble du secteur de la confiance numérique dans une dynamique positive.

M. Philippe Latombe, rapporteur. Merci à tous pour ces échanges, le temps que vous nous avez consacré et vos réponses.

Table ronde, ouverte à la presse, réunissant des représentants de la Confédération des petites et moyennes entreprise (CPME) : M. Alain Assouline, co-président de la commission « innovation et économie numérique », du Mouvement des entreprises de taille intermédiaire (METI) : M. Alain Conrard, président de la commission digitale, directeur général de Prodware Group, M. Sylvain Rouri, directeur des ventes d'OVHcloud, Mme Florence Naillat, adjointe au délégué général, M. Alexandre Bonis, responsable des affaires publiques, du Mouvement des entreprises de France (MEDEF) : M. Laurent Giovachini, président du comité « souveraineté et sécurité économique », président de Syntec et directeur général adjoint de Sopra Steria, M. Christian Poyau, co-président de la commission « mutations Technologiques & impacts sociétaux », co-fondateur et président-directeur général de Micropole, Mme Maxence Demerlé, directrice du numérique, Mme Stéphanie Tison, directrice adjointe à l'international au pôle économique, Mme Fadoua Qachri, chargée de mission à la direction des affaires publiques, Mme Clémentine Furigo, chargée de mission senior à la direction juridique
(14 janvier 2021)

Présidence de M. Jean-Luc Warsmann, Président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos travaux avec une seconde table ronde consacrée à la souveraineté numérique et à la commande publique. L'objectif de la mission d'information consiste à échanger avec des acteurs publics et privés afin d'examiner comment la commande publique peut servir à la transformation numérique de nos administrations, ainsi qu'à la construction d'une forme de souveraineté numérique nationale ou européenne.

Nous recevons par visioconférence M. Alain Assouline, coprésident de la commission « innovation et économie numérique » de la Confédération des petites et moyennes entreprises (CPME).

Pour le Mouvement des entreprises de taille intermédiaire (METI), nous accueillons M. Alain Conrard, directeur général de Prodware Group et président de la commission digitale du syndicat, M. Sylvain Rouri, directeur des ventes chez OVHcloud, Mme Florence Naillat, adjointe au délégué général du METI, M. Alexandre Bonis, responsable des affaires publiques du METI.

Représenteront le Mouvement des entreprises de France (MEDEF), M. Laurent Giovachini, président du comité « souveraineté et sécurité économique » de l'organisation patronale, président de la fédération Syntec, directeur général adjoint de Sopra Steria, M. Christian Poyau, coprésident de la commission « mutations technologiques et impacts sociétaux » du syndicat patronal, cofondateur et président-directeur général du groupe Micropole, Mme Maxence Demerlé, directrice du numérique, Mme Stéphanie Tison, directrice adjointe à l'international au pôle économique, Mme Fadoua Qachri, chargée de mission à la direction des affaires publiques, ainsi que Mme Clémentine Furigo, chargée de mission senior à la direction juridique.

Je vous souhaite la bienvenue, vous remercie de votre présence et des réponses écrites que vous nous avez déjà apportées ou que vous nous ferez parvenir.

M. Philippe Latombe, rapporteur. J'adresse les traditionnels vœux de début d'année, en espérant que 2021 effacera les stigmates de 2020.

À titre d'introduction à nos échanges, j'interrogerai les différents participants de la table ronde sur plusieurs sujets.

En premier lieu, que recouvre pour vous la notion de souveraineté numérique ? Depuis le déclenchement de la crise sanitaire, les pouvoirs publics lui accordent une attention croissante. Au cours de nos auditions successives, nous avons entendu plusieurs définitions de cette notion particulièrement large. Certains la rapprochent d'une forme d'autonomie stratégique ou décisionnelle. Le regard que vous portez, en tant qu'acteurs privés, sur ce concept m'intéresse. Selon vous, comment peut-il se traduire concrètement dans les politiques publiques ?

En second lieu, je souhaite recueillir votre avis sur la commande publique, thème principal de notre table ronde. Il s'agit d'un outil puissant, puisqu'il représentait environ 87,5 milliards d'euros en 2019, d'après le baromètre de l'Assemblée des communautés de France (AdCF) et de la Banque des territoires. Jugez-vous la commande publique suffisamment tournée vers des solutions numériques et technologiques françaises ou européennes ? Des petites et moyennes entreprises (PME) ou des entreprises de taille intermédiaire (ETI) portant certaines de ces solutions, pensez-vous qu'elles accèdent suffisamment facilement à la commande publique ? Dans le cas contraire, nous vous prions de nous préciser la nature des difficultés qu'elles rencontrent et entendrons avec intérêt vos propositions d'amélioration.

En dernier lieu, j'aimerais que nous abordions l'enjeu important de la numérisation des entreprises. Il se révèle des plus prégnants à l'occasion de la crise sanitaire. À ce sujet, nous soulèverons principalement deux interrogations. Comment d'abord inciter les entreprises à se numériser davantage, autrement dit à recourir à des outils numériques qui leur permettent d'être plus compétitives ? Comment ensuite développer une culture de la cyberprotection chez les acteurs privés, face à un risque croissant ? M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a récemment indiqué que le nombre des cyberattaques avait crû dans des proportions considérables en 2020, et a mis en avant une forte inventivité de la part des agresseurs.

Je vous laisse répondre à ces premières questions. Si nécessaire, nous les complèterons au fur et à mesure de la discussion.

M. Laurent Giovachini, président du comité « souveraineté et sécurité économique » du MEDEF, président de la fédération Syntec, directeur général adjoint de Sopra Steria. Avec M. Christian Poyau, nous sommes très heureux de participer à la présente table ronde, afin d'évoquer notre position au sein du MEDEF sur le sujet de la souveraineté numérique nationale et européenne, crucial pour le monde économique dans son ensemble. Notre propos liminaire abordera les trois points que vous avez soulevés.

Le MEDEF réunit 173 000 entreprises adhérentes, 91 fédérations professionnelles, 122 organisations territoriales. Je rappellerai que 95 % de ses entreprises adhérentes sont des très petites entreprises (TPE), des PME ou des ETI. Elles comptent en moyenne 47 salariés. Nous sommes donc directement concernés par la commande publique qui s'adresse aux PME et ETI.

Ainsi que vous l'avez mentionné M. le président, j'occupe les fonctions de directeur général adjoint de Sopra Steria. Forte de 45 000 collaborateurs présents dans 25 pays, générant

un chiffre d'affaires de 4,5 milliards d'euros, cette entreprise française est l'un des chefs de file européens de la transformation numérique. Comme d'autres, elle a subi en 2020 une cyberattaque d'ampleur. Si nous sommes parvenus à la parer à temps, elle ne nous en a pas moins causé certains dommages. Je puis donc témoigner de la recrudescence de ce phénomène de cyberattaques à l'occasion de la crise sanitaire et de la crise économique qu'elle provoque.

La fédération Syntec que je préside, rassemble dans ses syndicats affiliés des entreprises spécialisées dans les domaines, non seulement du numérique, mais également de l'ingénierie, du conseil, de la formation professionnelle et de l'événementiel. Elle représente 80 000 entreprises, un million de salariés, 8 % du produit intérieur brut français.

Enfin, j'interviens en qualité de président du comité « souveraineté et sécurité économique des entreprises » du MEDEF. Au sein de l'organisation patronale, nous n'avons pas attendu le déclenchement de la pandémie pour nous mobiliser sur les enjeux de souveraineté économique au sens large. À notre sens, la souveraineté numérique en forme l'un des volets.

Dès 2019, M. Geoffroy Roux de Bézieux, président de l'organisation, a souhaité la création d'un comité lié à ces thématiques. Dans un contexte international marqué par la rivalité commerciale entre les États-Unis, la Chine et d'autres puissances, avec l'emploi de législations extraterritoriales, tel le *clarifying lawful overseas use of data act*, ou *cloud act*, loi fédérale des États-Unis adoptée en 2018, face aux transformations numériques et technologiques, devant les enjeux climatiques, il est apparu indispensable que les entreprises françaises s'emparent des questions de souveraineté, de renforcement de leurs actifs et de leurs données.

À nos yeux, la démarche ne revêt nulle intention protectionniste. Elle vise simplement à se garder de toute candeur. Le libéralisme auquel nous demeurons attachés ne saurait être synonyme de naïveté. Il nous apparaît urgent d'affirmer nos ambitions de souveraineté et de nous donner les moyens, juridiques et financiers, de la préserver sur tous les plans. La souveraineté concerne aussi bien le numérique que les aspects technologiques, industriels, monétaires, juridiques, énergétiques et sanitaires. Nous entendons que nos entreprises expriment leurs talents à travers les frontières par le jeu de règles équitables, qu'elles prennent toute leur place dans la compétition internationale. Nous articulons la souveraineté selon un triptyque : protéger, ne pas entraver, rester attractif.

Nous nous félicitons de constater que le terme de souveraineté n'est désormais plus un tabou. Nous nous réjouissons que la prise de conscience des enjeux de souveraineté dans ses différentes dimensions, dont le numérique, se développe en France et en Europe. Ces enjeux se retrouvent dans les plans de relance nationaux et de l'Union européenne. Ils apparaissent dans l'ambitieux agenda que porte M. Thierry Breton, le commissaire européen au marché intérieur. À l'évidence, la crise sanitaire a accéléré cette prise de conscience, en particulier sur le rôle clé que jouent le numérique et ses acteurs.

Qu'il s'agisse de protection des données des entreprises, de régulation des acteurs du marché, de facilitation du recours à des outils sécurisés et à des technologies d'avenir, le MEDEF préconise une approche offensive du renforcement de notre souveraineté numérique. Celle-ci recouvre concomitamment les aspects régaliens, des intérêts économiques et des sujets de société.

Il en va de notre capacité à maîtriser notre destin. De ce point de vue, nous ne pouvons laisser les seuls États traiter la question de la souveraineté, notamment numérique. Il nous appartient de réduire nos dépendances, d'être plus autonomes, sans cependant verser dans

l'autarcie et sans nous couper des avancées techniques qui se développent au plan mondial et auxquelles nous entendons continuer d'avoir recours.

Il nous faut renforcer notre aptitude à affronter les crises, à « rebondir », à devenir plus « résilients », et nous donner les moyens d'une meilleure compétitivité sur les marchés internationaux. Nous refusons que nos entreprises dépendent uniquement des solutions d'un nombre excessivement restreint d'acteurs. La souveraineté vient soit de la maîtrise des techniques de pointe, soit de la diversité des sources d'approvisionnement.

En matière de souveraineté en général et de souveraineté numérique en particulier, nous recommandons une approche par cercles géographiques concentriques. Le ministère de l'économie, des finances et de la relance partage cette approche que nous lui avons soumise.

Le premier cercle inclut ce que nous devons impérativement maîtriser sur le territoire national en raison de l'importance des enjeux. Il s'agira par exemple des données les plus sensibles de certaines de nos administrations ou grandes entreprises.

Le deuxième cercle se rapporte au niveau européen et peut être soutenu par les initiatives européennes. À titre d'illustration, je citerai le projet Gaia-X dans le domaine du *cloud computing*, ou accès à des services informatiques via l'internet. Le MEDEF y adhère.

Le troisième cercle renvoie à ce qui autorise des partenariats internationaux extra-européens, en vue de répondre aux besoins de développement de nos entreprises que je qualifierai de « standards ». Je répète qu'il n'est pas question de nous couper des acteurs non européens qui détiennent des techniques importantes.

L'approche que je vous décris ne se matérialisera que si elle repose sur des partenariats public-privé plus étroits qu'ils ne le sont à présent. Ces partenariats ne se restreignent pas aux seules commandes publiques. Il m'importe que nous analysions comment des partenariats entre les secteurs public et privé ont progressé dans d'autres domaine que le numérique. Je pense à celui qui a cours aux États-Unis pour l'élaboration de vaccins contre le coronavirus.

Outre la commande publique, le succès de tels partenariats semble lié chez nous à la capacité à mettre en œuvre, fort en amont, des politiques d'investissement auprès d'acteurs privés, certes à l'échelle nationale, mais peut-être aussi, voire surtout, à celle de l'Union européenne. Avant qu'il ne soit trop tard, il revient à la puissance publique de prendre le risque de miser sur des solutions numériques nationales ou européennes. À l'extérieur de l'Europe, des gouvernements excellent en la matière. Imitons-les. De ces partenariats dépend l'émergence de compétiteurs français et européens auxquels il sera loisible de confier nos commandes publiques.

M. Christian Poyau complétera mes propos.

M. Christian Poyau, coprésident de la commission « mutations technologiques et impacts sociétaux » du MEDEF, président-directeur général de groupe Micropole. Je m'attacherai à la numérisation des entreprises.

Moi-même entrepreneur, j'ai fondé et dirige la société Micropole. Elle compte environ 1 200 salariés et, présente dans six pays, réalise à l'export 36 % de son chiffre d'affaires annuel de 115 millions d'euros. Je suis parmi vous au nom de la commission « mutations technologiques et impacts sociétaux » du MEDEF, à laquelle j'appartiens depuis plusieurs années. De fait, voilà cinq ans que le MEDEF a pris à bras-le-corps le sujet de la numérisation des entreprises.

Celle-ci s'avère un vecteur majeur de l'accélération de la productivité et de la compétitivité, ainsi que de la création d'emplois. Nous agissons donc résolument pour sa promotion.

Chacun le constate : la crise sanitaire a mis en avant l'utilité des outils numériques. J'évoquerai quelques secteurs.

La télémédecine a connu une accélération de son développement évaluée à deux années. Entre les mois de mars et avril 2020, l'assurance-maladie a remboursé 5,5 millions de consultations effectuées à distance. Le système permet un service d'une qualité indéniable, plus rapide. Il contribue à désenclaver certains territoires, tout en restant moins onéreux pour la collectivité.

Le télétravail a concerné quelque 27 % des personnes en activité. Il a entraîné un changement des habitudes et des mentalités. Nous verrons comment il continuera d'exister. Difficile à organiser, il requiert que nous l'adaptions aux attentes et besoins de nos collaborateurs.

Les sites d'achat en ligne avec un service de retrait des commandes en magasin, dit de *click and collect*, se sont par ailleurs multipliés.

Nonobstant des critiques qui concernent notamment ses conséquences sur l'environnement, le numérique emporte d'indéniables effets positifs sur la qualité de vie de nos collaborateurs et de nos concitoyens.

Dans son plan de relance, le Gouvernement prévoit un volet relatif à la numérisation des entreprises, pour un montant de 385 millions d'euros. Nous le jugeons clairement insuffisant et pour le moins limité en comparaison de l'investissement total que le plan représente.

Le volet se compose pour partie d'une sensibilisation à la numérisation. Mon expérience du terrain me permet d'affirmer que les entreprises sont d'ores et déjà parfaitement conscientes de la nécessité de leur numérisation.

Il comprend également un dispositif d'audit et d'accompagnement. Nous regrettons que celui-ci se polarise sur le secteur industriel. S'il s'avère utile d'aider les industries françaises à améliorer leur numérisation, il convient de n'en pas négliger pour autant le secteur des services.

J'ajoute que nos structures, dont le MEDEF Île-de-France, nous ont signalé que, faute de fonds disponibles, l'aide du plan de relance à l'investissement de transformation vers l'industrie du futur serait ramenée de 40 %, ainsi qu'initialement prévu, à 10 % du coût de l'investissement engagé. La surprise et l'inquiétude des entrepreneurs en sont vives. L'annonce suscite l'interrogation de ceux qui avaient commencé à établir des prévisions sur le fondement du plan de relance.

Sur les aspects de cybersécurité, je conviendrai que toutes les entreprises se trouvent sous la menace d'attaques informatiques. Même si le respect de règles fondamentales de sécurité demeure essentiel, aucune parade ne permet de les en prémunir définitivement. Nous œuvrons plutôt à communiquer sur la réaction à adopter en cas d'attaque. Malheureusement, sous l'angle du droit, les moyens dévolus à la justice sur les questions qui tiennent au numérique, apparaissent dérisoires.

La dernière partie de mon intervention traitera des données, avant de conclure sur la commande publique.

La numérisation des entreprises, que j'évoquais à l'instant, a mis en avant le poids des plateformes en ligne. Elles sont le plus souvent d'origine extra-européenne. Il nous semble qu'une compétition commerciale équitable implique de disposer d'armes égales à celles de la concurrence.

Le combat n'est pas perdu. Les plateformes ne vivent que des données que nous leur confions. Gardons à l'esprit que l'Europe constitue le premier marché économique mondial des données informatiques. Or, sur notre continent, leur accès reste à ce jour ouvert sans aucune espèce de contrainte.

Par le jeu d'une action de souveraineté, sans agressivité, mais sans ingénuité non plus, une volonté ferme de protéger nos données nous permettra sans conteste de beaucoup progresser.

Déjà cité, le projet Gaia-X s'engage dans cette voie. Il vise l'interopérabilité et la portabilité des données. Je mentionnerai également les *data hubs*, ou centres de données. Des initiatives les concernent, par exemple dans le domaine de la santé. Il faut les y étendre à la partie industrielle, celles des données partagées entre professionnels, en « *B to B* » (*business to business*).

Lorsque nous évoquons les partenariats entre les secteurs public et privé, nous pensons notamment à l'entreprise américaine SpaceX. Celle-ci doit sa réussite au soutien que la *national aeronautics and space administration* (NASA) lui apporte par son financement. Dans cet exemple, un État oriente ses investissements vers un acteur privé, dont il autorise ainsi une dynamique forte. Amazon Web Services (AWS), acteur mondial de premier plan dans le domaine du *cloud*, a de même bénéficié, dans les années 2000, du levier d'un investissement de la *defence advanced research projects agency* (DARPA) de 500 millions de dollars.

Le secteur privé ne manque pas de dynamisme, d'inventivité, ni d'ambition. Il appartient à nos autorités de l'encourager par ses financements, le plus en amont possible de la commande publique. Notre plan de relance national ne considère pas assez le problème de la numérisation des entreprises, mais entretenons une attitude positive. Rien n'est encore perdu pour la France et l'Europe dans ce domaine. Par une coopération étroite de leurs institutions avec le secteur privé, elles disposent des moyens d'y faire entendre leur voix et d'en relever les défis.

Mme Florence Naillat, adjointe au délégué général du METI. Au nom du METI, je vous remercie pour votre invitation à nous exprimer devant votre mission d'information.

Le METI fédère et représente les entreprises de taille intermédiaire. La France dénombre 5 400 ETI, essentielles à l'ossature économique et sociale de ses régions. Pour les deux-tiers d'entre elles, les ETI disposent d'un siège social situé en dehors de l'Île-de-France. Elles fournissent 25 % des emplois en général, 38 % de ceux de l'industrie manufacturière. De 2009 à 2015, après la crise économique de 2008, cette catégorie d'entreprise a démontré sa capacité de résistance, avec la création nette de 335 000 postes, devenant pendant la période la principale pourvoyeuse d'emplois. Les ETI s'ouvrent particulièrement à la scène internationale. Ne constituant que 4 % des exportateurs, elles assurent 34 % des exportations nationales et pour les trois-quarts d'entre elles sont présentes en dehors de nos frontières.

En dépit de leurs atouts, la crise que nous traversons les affecte durement. Nous attendons encore les résultats consolidés de 2020. Toutefois, avec des disparités selon les secteurs d'activité, nous en estimons l'évolution moyenne du chiffre d'affaires en 2020 à une baisse de l'ordre de 8 %. Plus de la moitié a connu une dégradation de sa capacité d'investissement et de son ratio entre endettement et fonds propres. Plus de quatre sur dix d'entre elles ont dû consentir à une diminution de leur effectif au cours de l'année. Enfin, en 2020, une ETI sur dix a fait l'objet d'une tentative de rachat étrangère et, dans la même proportion, d'une tentative étrangère d'entrée dans son capital. Un risque assez élevé de prédation les touche actuellement.

Au regard du sujet qui nous occupe, ces éléments conjoncturels nous indiquent qu'afin de relever les défis de la transformation et de la souveraineté numériques, les ETI requièrent un environnement concurrentiel favorable. C'est pourquoi le METI plaide de longue date en faveur de mesures structurelles de compétitivité, à l'instar de celles que le plan de relance français intègre, au premier rang desquelles une baisse de la fiscalité applicable à l'activité productive.

M. Alain Conrad propose de vous dresser un état des lieux de la maturité numérique des ETI, à la lumière d'un baromètre que nous avons récemment publié.

M. Alain Conrard, président de la commission digitale du METI, directeur général de Prodware Group. Président de la commission digitale du METI, je dirige la société Prodware. Créée en 1989, celle-ci accompagne, au service de leur compétitivité, les entreprises dans la fourniture de leur système d'information. Depuis une dizaine d'année, nous nous positionnons toujours davantage sur les aspects de transformation numérique des entreprises qui nous accordent leur confiance. Prodware est présente dans quatorze pays. Elle enregistre un chiffre d'affaires de 190 millions d'euros, dont 60 % sont réalisés à l'international.

Nous possédons donc les résultats d'une étude que le METI a commandée à l'institut de sondages CSA en septembre 2020 sur la maturité numérique des ETI, en s'associant au cabinet Ernst & Young et associés (EY) et à la société d'investissement Apax Partners. Certaines des informations qu'elle révèle nous paraissent mériter votre attention.

Il en ressort que la maturité numérique des ETI progresse. Deux ETI sur trois se sont activement engagées dans leur transformation numérique. La crise sanitaire en a à l'évidence accéléré le processus en modifiant l'organisation du travail à l'intérieur des entreprises. Dans 92 % des cas, les ETI ont, dans ces circonstances, accentué leur recours aux outils numériques, qu'il s'agisse par exemple de messageries instantanées, d'applications de visioconférence ou de transfert de fichiers informatiques. Nous relevons que 84 % des décideurs de ces entreprises s'estiment désormais en mesure d'affronter les conséquences de la crise que nous traversons.

L'étude rapporte également un investissement toujours plus massif des ETI dans le numérique. Leur investissement concerne essentiellement la modernisation des infrastructures, l'acquisition d'outils numériques collaboratifs, le déploiement d'outils d'amélioration de l'« expérience client », ceux de marketing numérique, de commerce en ligne et la cybersécurité. Pour 71 % d'entre eux, les dirigeants interrogés déclarent vouloir poursuivre leurs investissements dans les solutions numériques.

L'âge moyen d'une ETI est de 31 ans. Ces sociétés font montre d'un fort pragmatisme dans le choix de leurs priorités d'investissement. Elles calculent d'abord leur retour sur investissement. Ceux qu'elles opèrent de nos jours montrent sans ambages l'importance qu'elles accordent aux outils numériques.

La manière d'aborder la transformation numérique dans les entreprises revêt par ailleurs un caractère décisif. L'étude dévoile que 71 % des ETI estiment que leurs direction générale et direction des systèmes d'information (DSI) portent principalement la transformation numérique en leur sein.

En pratique, cette transformation se heurte à plusieurs obstacles : la résistance au changement, le défaut de vision partagée, des difficultés à intégrer les nouvelles compétences, la nécessité que les décideurs appréhendent les conséquences profondes de la transformation sur leur entreprise. Je pense ici à celles de l'intelligence artificielle, des mégadonnées (*big data*), ou de l'internet des objets (*IoT*), sur l'organisation et le modèle même des entreprises, leurs canaux et modes de production. Les ETI n'investissent pas encore assez dans ces sujets qui déterminent pourtant en partie leur performance future.

Il est vrai que la crise sanitaire intervient après une première période difficile pour elles, marquée par les effets de mouvements sociaux éprouvants, ceux des « gilets jaunes » et de grèves nationales. Ces épreuves successives n'améliorent guère leur capacité de financement.

En conclusion, il nous paraît essentiel que les ETI continuent d'accélérer leur transformation numérique. À mesure que celle-ci se concrétise, ses enjeux apparaissent avec plus de netteté, notamment en matière de sécurité et de souveraineté. La récente étude du courtier Bessé montre que 76 % des dirigeants d'ETI ont subi au moins une incidence cyber en 2019 et 2020. La question reste de savoir comment les aider au mieux dans le choix et la mise en œuvre de solutions appropriées.

M. Sylvain Rouri, directeur des ventes d'OVHcloud. J'exerce les fonctions de directeur exécutif chez OVHcloud. Installée dans le nord de la France, cette société occupe, avec 1,6 million de client, la première place parmi les acteurs européens du *cloud*. Elle compte plus de 2 400 employés répartis dans le monde. Elle réalise 60 % de son chiffre d'affaires à l'étranger.

Le METI porte toute son attention à la question de la souveraineté numérique. Il en retient une approche en deux temps, en distinguant entre souveraineté des données et souveraineté technologique.

La première doit permettre aux dirigeants d'entreprise de comprendre la portée précise de leurs choix en matière de stockage de leurs données, de mesurer l'exacte étendue de leur utilisation par l'acteur auquel ils s'associent. Ici, le METI promeut information et formation, afin que les décisions se prennent en toute connaissance de cause, en toute transparence et en pleine liberté.

Nous constatons que la donnée se déplace d'un continent à l'autre, sans que l'utilisateur du service en soit systématiquement averti, et pour des usages qui ne sont pas nécessairement ceux auxquels il a souscrit. Il s'avère urgent que les Européens reprennent le contrôle de leurs données. De notre point de vue, aucun compromis ne saurait grever la souveraineté de ces données.

La souveraineté technologique sous-tend l'idée d'une autosuffisance dans la maîtrise technologique. À ce jour, force est de constater qu'éloignée de la réalité, elle demeure un vœu pieux. À maints égards, nous dépendons de solutions étrangères. Dans ces conditions, nous n'incitons pas à un quelconque repli dans la recherche de solutions strictement souveraines. Notre propos encourage au contraire à rester ouvert.

Nous mettons donc l'accent sur le premier aspect de la souveraineté numérique, celui de la souveraineté des données. Dans le processus de numérisation des entreprises, nous souhaitons qu'un nombre toujours croissant de dispositifs aident les entrepreneurs à comprendre pour mieux choisir. L'ANSSI y contribue par les certifications qu'elle met en place. Il importe désormais d'en ouvrir l'accès aux entreprises de la manière la plus large possible.

Ne perdons pas de vue que pour une entreprise, choisir une plateforme dédiée aux ressources humaines engage les données tant privées que professionnelles de ses collaborateurs, selon des principes qui peuvent relever d'une réglementation autre que nationale. Je doute que tous les entrepreneurs français en aient une claire conscience lorsqu'ils décident de recourir à telle ou telle plateforme. Conférer un label de confiance souverain aux plateformes et logiciels contribuerait à les éclairer dans leur choix.

Quant à la commande publique, elle semble des plus insuffisantes sous l'angle de la souveraineté de nos données. Elle n'insuffle pas le mouvement qui nous conduirait à en reprendre le contrôle de la valeur et des atouts qu'elles représentent. Je ne reviendrai pas sur la décision que des institutions publiques ont prise de recourir à des plateformes étrangères dans des domaines où, pourtant, l'information s'avère sensible. Je préfère évoquer la marge de progression qu'il nous reste à combler.

Je souscris pleinement à l'idée d'un partenariat entre le secteur public et le secteur privé, très en amont de la commande publique. Le travail de recensement, de labellisation, de certification doit ici permettre au secteur public de mieux connaître les acteurs en présence.

Nous constatons une méconnaissance totale des compétences et des savoir-faire des entreprises de la « tech » française. Elle en contrarie nombre d'initiatives et en provoque parfois le départ dans le sillage d'investisseurs étrangers.

Il importe que la commande publique gagne en importance et montre l'exemple. En 2018, l'État a effectué un travail remarquable en segmentant en trois « cercles » l'approche du *cloud* et des offres qui le concernent. Cependant, à ce jour, seul s'est matérialisé le premier de ces cercles, qui vise à répondre à des besoins strictement régaliens d'infrastructures numériques. Poursuivons résolument cet effort. Les propositions ne manquent pas pour rapprocher et valoriser les savoir-faire français et européens au service d'une numérisation qui nous ménage la maîtrise de nos données et contribue au rayonnement de nos entreprises.

M. Alain Assouline, coprésident de la commission « innovation et économie numérique » de la CPME. Je préside la commission numérique de la CPME, ainsi que CINOV-Numérique, le syndicat des petites entreprises du numérique. Par ailleurs, je dirige le réseau des écoles WebForce3 que j'ai fondé. Il forme aux métiers du numérique dont nous avons besoin.

La CPME regroupe 1,5 million d'entreprises adhérentes, qui représentent trois millions de salariés.

L'éclosion de l'internet portait avec elle des promesses de liberté. L'outil était supposé lever barrières et frontières. Nous nous sommes cependant aperçus qu'un espace non réglementé emportait également la possibilité de maux considérables.

En Europe, dans les années 2000, la question de la souveraineté numérique s'est ainsi d'abord posée sous l'angle de la réglementation, en particulier à l'égard des données personnelles.

Assurer cette souveraineté se révèle aujourd'hui nécessaire à la bonne marche de l'économie européenne, à la liberté des individus et des entreprises. Il s'agit principalement de garantir la libre circulation des données dans une situation où le plus fort risque d'imposer ses vues.

Le numérique demeure un secteur complexe. Stimulant de prime abord l'innovation, il peut également produire des effets de réseaux préjudiciables à la fertilité de l'économie. Des acteurs s'ancrent dans des positions durables sur ce marché du numérique, à l'entrée duquel ils établissent des barrières. Nos petites entreprises, qui n'en peuvent guère discuter les conditions, en deviennent dépendantes.

Au sein de la CPME, nous pensons que PME et TPE assurent une fonction primordiale dans l'économie. Toutefois, pour assurer leur rôle, il leur faut jouir d'un environnement favorable à une concurrence loyale et à l'innovation. L'indépendance numérique vis-à-vis d'États tiers et d'entreprises dominantes devient un gage d'efficacité et de sécurité dans les activités qu'elles mènent. La souveraineté numérique prend pour elles d'autant plus de sens qu'elle rétablit une libre concurrence et des conditions d'innovation optimales.

Reconnaissons que nous nous tenons encore fort éloignés d'une souveraineté numérique française ou européenne. Quoique nous adoptions des mesures sur les questions de maîtrise de nos données et de régulation, les principales entreprises mondiales du secteur numérique, tant sur les aspects de matériel qu'en matière de logiciels, ne sont pas européennes. Aucun opérateur européen ne figure parmi elles. Il en ressort une certaine dépendance à l'égard des entreprises américaines et asiatiques.

Les téléphones mobiles utilisent exclusivement les systèmes d'exploitation Android ou iOS. Les grandes plateformes numériques exercent une forme de monopole sur les marchés des moteurs de recherche. Il leur permet de contrôler le référencement des sites en ligne. Par les conditions commerciales qu'elles imposent, ces mêmes plateformes créent également la possibilité d'une dépendance à leurs services.

Les TPE et PME se révèlent particulièrement vulnérables à de telles pratiques, du fait du taux élevé de leur recours à des services en ligne. Selon la Commission européenne, ce taux atteint 42 % et s'avère majoritairement lié à l'utilisation des moteurs de recherche.

Comment les pouvoirs publics pourraient-ils promouvoir une souveraineté numérique française et européenne ? Outre l'attention à porter à la formation de nos chefs d'entreprise, nous pensons que la manière la plus efficace d'y parvenir consisterait à privilégier une réglementation favorable à l'émergence de nos propres grands acteurs du numérique. Ne nous avouons pas vaincus et, par l'organisation de réglementations adaptées aux entreprises, particulièrement aux PME, encourageons l'émergence de ces nouveaux acteurs.

De plus, nous estimons nécessaire de réglementer plus rigoureusement les plateformes actuelles. À l'évidence, si elles paraissent dans un premier temps proposer aux TPE et PME françaises des solutions séduisantes pour la promotion de leurs produits et de leur image commerciale, elles préjudicient ensuite à leur développement et représentent une forme d'impasse.

La CPME salue l'initiative de la Commission européenne qui a conduit à l'adoption de deux règlements, l'un sur les services numériques, l'autre sur les marchés numériques. Ils remettent en question les effets de réseaux, la position dominante et durable de certains acteurs. En s'attaquant au comportement de plateformes qui agissent en tant que « contrôleurs

d'accès » sur les marchés numériques, ces textes sont susceptibles de contribuer à l'amélioration de la capacité des TPE et PME à suivre le rythme de la transition numérique.

À notre avis, promouvoir la souveraineté numérique passe pour beaucoup par l'encouragement des entreprises à utiliser des outils européens et français. De cette manière, nous favoriserons l'émergence, sur notre continent, d'acteurs de premier plan du secteur numérique. Du moins, il importe que nous aidions, par nos financements, nos entreprises à se développer sans recourir systématiquement aux outils étrangers.

L'hébergement de nos données en Europe s'avère essentiel, afin d'assurer leur sécurité et notre entière liberté dans leur utilisation. À ce titre, pour se prémunir des dangers potentiels, il apparaît utile d'organiser des campagnes de sensibilisation et de formation au sein des entreprises sur la notion de souveraineté numérique.

PME-TPE, citoyens et pouvoirs publics doivent œuvrer de concert. Par-delà les mesures, nous jugeons primordial le comportement général des citoyens. Ils représentent la masse des utilisateurs et leurs choix pèsent sur les évolutions du marché. Si nous voulons y prendre une place, il nous revient de les convaincre. Pour l'obtenir, protéger ne suffit pas : il nous faut être les meilleurs.

Nous remarquons la propension de certains États à capter les données afin d'affermir leur puissance économique. À ce jour, plus de 90 % des données disponibles ont été produites au cours des deux dernières années. Le fort développement de l'économie des données a pour corollaire l'importance croissante des enjeux éthiques et sécuritaires.

Une place reste à prendre. Elle ne consiste sûrement pas à imiter Chinois et Américains. L'Europe gagnera à s'inspirer de ses valeurs propres et à bâtir un modèle original.

En raison de son poids économique, de l'ordre de 8 % du produit intérieur brut français, la commande publique joue un rôle non négligeable. La question de la territorialisation de cette commande, avec la valorisation des savoir-faire locaux, partant la question de la place accordée aux PME, ne manque pas d'importance.

Les PME demeurent sous-représentées dans l'achat public. Selon l'observatoire économique de la commande publique (OECP), si elles ont été attributaires de 57 % des marchés conclus en 2017, les contrats qu'elles obtiennent ne représentent que 29 % du montant total de ces marchés. Or, comme le rappelait l'un des intervenants du MEDEF, elles constituent 95 % de notre tissu d'entreprises.

L'explication en tient aux limites de leur capacité financière, au problème des délais de paiement, à l'absence ou à l'insuffisance d'avances, enfin à la complexité des procédures d'appel d'offres, ainsi qu'aux délais parfois excessivement brefs de ces dernières. Récemment, les pouvoirs publics ont pris des mesures destinées à améliorer la situation des PME. Elles n'en connaissent pas moins un durcissement de leurs relations avec les établissements bancaires.

La CPME se prononce en faveur d'une relance massive de la commande publique sur des enjeux stratégiques. Le plan du Gouvernement pourrait y aider. Néanmoins, je partage l'analyse selon laquelle il consacre une part trop restreinte à la transformation numérique, notamment pour ce qui a trait aux PME.

Une telle relance suppose une politique publique effective qui permette aux acheteurs de mieux orienter leurs choix, en tenant certes compte de critères techniques, mais aussi de

critères de qualité sociale ou environnementale, avec la préférence pour des circuits courts. Des dispositifs existent, par exemple celui du label « relations fournisseurs et achats responsables ». Ils paraissent cependant mal connus des acheteurs publics, qui les mettent peu en application.

Le soutien de la puissance publique concerne également la numérisation des entreprises. Nous avons eu l'occasion de lui signaler que le montant d'environ 300 millions d'euros qu'elle lui alloue se révèle notoirement insuffisant. En partenaires loyaux, nous avons néanmoins réfléchi à la manière de l'employer au mieux.

Nous ne concevons nullement la sensibilisation aux enjeux numériques comme une injonction à la transformation numérique. Parties prenantes des formations-actions qui s'élaborent, nous croyons plutôt à la nécessité de poser pour point de départ les problématiques et besoins des entreprises, afin que le numérique leur apparaisse comme une solution.

En Europe, loin du rang économique qui lui revient, la France n'occupe que la seizième place s'agissant de la transformation numérique des TPE-PME. La CPME a engagé un tour de France, afin de se rapprocher des territoires et d'accompagner au plus près les petites entreprises qui les animent. De fait, ce n'est le plus souvent pas dans les principales métropoles que la transformation numérique s'avère lacunaire.

Ces petites entreprises peinent à définir leur voie parmi la multiplicité des solutions qui s'offrent désormais à elles. La plateforme France Num témoigne du nombre et de la diversité des aides existantes. Nous défendons de longue date l'idée d'un guichet unique à destination des chefs d'entreprise. Ils y trouveraient un point d'accès à l'ensemble des informations qui les intéressent sur les accompagnements dont ils peuvent bénéficier.

En ce sens, nous nous inspirerions opportunément de l'exemple allemand, celui d'un programme national d'envergure, le *Kompetenzzentrum Digitales Handwerk*. Il propose un éventail complet de services dédiés à la transformation numérique des artisans et des TPE. Il s'adresse aux PME afin de les accompagner dans la voie de la numérisation, en mettant en exergue le potentiel technique et économique que celle-ci renferme pour elles. Il démontre son efficacité.

Pour notre part, le tour de France que nous avons entrepris entend de même montrer aux entreprises le bénéfice concret qu'elles tireraient de leur numérisation. En la matière, tout accompagnement n'obtiendra de succès que s'il pourvoit à leur fourniture en outils immédiatement utiles et mobilisables. En tant que telle, la sensibilisation ne suffit pas. À partir des problématiques qui se posent, il faut sans délai l'assortir de solutions concrètes.

La crise sanitaire de 2020 a, pour nombre d'entreprises, marqué le début de leur transformation numérique. Devant notamment recourir à des solutions de type *click and collect*, elles s'y sont parfois engagées dans un certain désordre et sans réelle méthode. Par effet de symétrie, les cyberattaques ont cru de 400 % pendant la période. Les formations-actions se destinent à aider nos entreprises à mieux conduire leur transformation numérique. Les enjeux de cybersécurité y occupent une place prépondérante, tant ils nous semblent une composante essentielle, non seulement de la souveraineté, mais également de la confiance que les entrepreneurs mettent dans le processus et, par suite, l'une des clés de sa réussite.

Vous nous aviez par ailleurs interrogés sur des aspects de concurrence et de fiscalité numériques. À l'évidence, la réflexion sur la souveraineté numérique ne saurait les omettre. Il paraît difficilement acceptable que des géants du numérique qui tendent à écraser la

concurrence, échappent dans une large mesure à leurs obligations fiscales. Nous plaidons en faveur de la transparence de leurs activités et des profits qu'ils en retirent sur notre territoire.

Étant donné le retard que les PME et TPE françaises ont pris dans la réalisation de leur transformation numérique, il conviendrait de dédier à cette transformation un budget spécifique, géré par un organe unique, par exemple l'agence du numérique rattachée au ministère de l'économie, des finances et de la relance. Il a été proposé de flécher vers lui la totalité des recettes de la fiscalité des géants du numérique, les « GAFA » (Google, Apple, Facebook, Amazon).

M. Philippe Latombe, rapporteur. À l'occasion de la précédente table ronde de ce jour, des représentants d'entreprises du secteur de la cybersécurité ont préconisé une forme de certification ou de labellisation obligatoire à laquelle les acheteurs publics se référeraient. D'une part, elle les assurerait de la robustesse des systèmes et des produits numériques qu'ils sont susceptibles d'acquérir. D'autre part, elle les acculturerait au recours à des solutions qui répondent aux normes et valeurs européennes. Elle suppose une nécessaire modification de la réglementation. En jugez-vous la proposition pertinente ? Vous paraît-elle induire une promesse d'efficacité ou, à l'inverse, présenter le risque d'une complexité accrue ?

M. Laurent Giovachini. L'ANSSI s'est déjà engagée dans une démarche de labellisation. Son directeur général a dû vous l'indiquer.

M. Philippe Latombe, rapporteur. Les intervenants qui vous ont précédés entendaient renforcer encore l'approche de certification qui prévaut actuellement.

M. Laurent Giovachini. Il est en effet envisageable d'aller plus avant, mais il conviendrait d'abord de bien exploiter les labels existants. Je pense par exemple à ceux des prestataires de détection d'incidents de sécurité (PDIS) ou de prestataires de réponse aux incidents de sécurité (PRIS). Ils donnent l'occasion de mettre en valeur des acteurs de confiance, pour l'essentiel français, notamment en raison de la réponse qu'ils apportent aux cyberattaques ou des audits de sécurité qu'ils mènent à titre préventif.

La cybersécurité forme la première brique de l'assise de la souveraineté numérique. C'est vraisemblablement dans ce domaine que nous sommes les moins démunis. À l'œuvre, la démarche de labellisation y porte ses fruits. Sans doute les enjeux de souveraineté numérique se posent-ils avec davantage d'acuité au-delà de ce socle de la cybersécurité.

L'un de nos interlocuteurs a proposé de distinguer entre souveraineté des données et souveraineté technologique. La distinction qu'il opère me convient. Néanmoins, quoique le premier type de souveraineté revête un caractère essentiel et dépasse les seuls aspects de cybersécurité, je ne crois pas que des acteurs français et européens aient perdu toute chance de s'imposer en matière de technologie et de souveraineté technologique.

Évidemment, en Europe, nous ne possédons ni GAFA ni BATX (Baidu, Alibaba, Tencent, Xiaomi). Pourtant, notre écosystème de *startups*, d'entreprises de services numériques telles que Capgemini, Atos, Sopra Steria, d'éditeurs de logiciels comme Dassault Systèmes ou l'allemand SAP, d'hébergeurs à l'instar d'OVHcloud, de sociétés stratégiques particulièrement concernées par le numérique, par exemple Thales, porte les germes de champions susceptibles d'aider les États européens, non seulement à répondre au problème des cyberattaques et à préserver la souveraineté de leurs données, mais aussi à assurer une forme de souveraineté technologique dans le domaine numérique.

À l'échelon européen, nous sommes parvenus, quelques années en arrière, à réagir contre l'omniprésence du système américain de géopositionnement par satellites, le GPS. Fondé sur l'excellence spatiale française et européenne, le programme Galileo permet progressivement de n'en plus dépendre totalement.

Dans le domaine numérique, nous évoquions l'initiative Gaia-X. Citons celle que la Commission européenne vient de lancer en ce mois de janvier 2021, dénommée Hexa-X. Elle consiste en un projet de recherche dans le domaine des réseaux sans fil 6G, en partenariat avec l'entreprise finlandaise Nokia.

Au commencement de la téléphonie mobile, au début des années 1990, Français et Européens étions, avec la norme GSM, les premiers mondiaux. Nous avons ensuite, petit à petit, perdu notre avance. Nous voyons ce qu'il en est de nos jours avec la cinquième génération (5G) de standards pour la téléphonie mobile. En prenant le risque d'investir, l'Europe s'efforce désormais d'être présente, en 2030, au rendez-vous de la 6G.

Labelliser dans le domaine de la cybersécurité reste positif. Pourtant, il ne s'agit que d'une première étape. Elle est certes essentielle puisque les risques de cyberattaques s'amplifient à mesure que la société se numérise. Plus avant de la question de la protection et, surtout, de l'hébergement des données, ne nous estimons pas vaincus sur le plan de la souveraineté technologique.

Si personne ne niera qu'il nous faut continuer d'accéder aux technologies qui se développent en dehors de notre continent, ne nous interdisons pas de susciter l'émergence de nos propres protagonistes. Notre tissu industriel et de services nous autorise à fonder quelque espoir dans le succès de l'entreprise, au moins dans le domaine du *B to B*, le numérique pour l'industrie. Il est vrai que les plateformes chinoises et américaines paraissent pour l'heure solidement implantées dans celui de la relation entre professionnels et particuliers, ou « *B to C* » (*business to consumer*). Je demeure optimiste devant les initiatives françaises et européennes. Nous disposons des moyens de remonter la pente et la partie n'est pas perdue d'avance.

M. Alain Assouline. Je partage cet avis. Dans le secteur du numérique, les positions des uns et des autres évoluent dans des délais extrêmement courts. Pour ce qui tient à l'usage même du numérique, l'Europe n'a pas pris de retard. Il est exact que nous comptons des acteurs de renom parmi les entreprises de services numériques (ESN, anciennement sociétés de services en ingénierie informatique, SSII) ou les éditeurs.

Pour autant, je veux attirer votre attention sur le risque qui consisterait à abandonner aux géants actuels, les GAFA, tout le secteur de la grande consommation. Précisément, étant le principal producteur de données, ce secteur pose le premier la problématique de notre souveraineté numérique.

À ce sujet, je ne sais dans l'immédiat suggérer de solution. Je considère néanmoins qu'il nous faut collectivement réfléchir à un modèle numérique alternatif qui prenne appui sur nos territoires et leurs valeurs, nos PME et notre agilité.

Je regrette le temps que nous avons perdu. En dépit des fleurons de notre industrie informatique, nous nous sommes laissé dépasser sur le terrain de la grande consommation et des usages du quotidien, ceux de la téléphonie mobile, des réseaux sociaux, des plateformes en ligne, des places de marché électroniques. Avec la crise sanitaire, nombre de nos commerçants, TPE et PME, ont entrepris leur transformation numérique. Bien souvent, ils

n'ont d'autre choix que ceux que leur proposent des acteurs étrangers, tels que Facebook et Amazon.

Ne pas nous imposer dans le registre de ces usages généralisés du quotidien rendrait vaine notre réaction sur les questions de souveraineté numérique. Montrons-nous offensifs également sur ce terrain.

M. Christian Poyau. Un acteur comme Amazon tire son avantage de la qualité des usages qui ont cours avec, en arrière-plan, le déploiement d'une chaîne logistique. Seule une volonté commune des acteurs européens d'investir massivement dans l'amélioration de l'expérience utilisateur, l'UX (*user experience*), contrebalancera les équilibres actuels du marché numérique grand public.

Notons au passage qu'en matière d'offre numérique dans le secteur de la distribution alimentaire, des acteurs comme Leclerc ou Auchan conservent en France une position de tête.

Je reviendrai un instant sur les aspects de certification. Nous y relevons dès à présent de nombreuses réalisations. Je doute qu'en ajouter améliorerait la situation qui nous occupe. Il convient de ne pas oublier que toute nouvelle certification équivaut pour les PME à des contraintes, et à autant de barrières, supplémentaires. Concentrons-nous sur d'autres sujets.

Sur celui du plan de relance en particulier, notre organisation professionnelle propose un crédit d'impôt à la numérisation, ainsi qu'à la transition énergétique et environnementale. Aidons les entreprises françaises à investir dans ces domaines. Pour l'heure, une rentabilité communément inférieure à celle de leurs concurrents les y entrave.

Par ailleurs, la transformation des entreprises tient à la conduite du changement et à la formation. Des investissements tant publics que privés doivent également s'y intéresser.

M. Sylvain Rouri. Il importe en effet que la certification ne devienne pas une contrainte additionnelle dans l'accès de nos entreprises aux marchés publics. Cependant, je prétends qu'il nous faut progresser, sinon dans la certification, du moins dans la qualification, et associer la souveraineté des données à la cybersécurité. Dans les dispositifs existants, la notion de souveraineté des données reste encore trop peu mise en avant.

Une tendance simpliste tend à affirmer que la partie est perdue sur le terrain de la donnée personnelle et que l'Europe doit désormais s'attacher à remporter celle de la donnée professionnelle. Pour notre part, nous pensons que la seconde prolonge essentiellement la première. C'est pourquoi nous invitons à notre tour à ne pas nous avouer vaincus. L'éclairage de la certification et de la qualification offre un moyen efficace de promouvoir l'exigence de souveraineté des données.

En outre, je partage l'idée selon laquelle un important effort d'accompagnement des PME-TPE demeure à réaliser prioritairement. Nombreuses en France, elles connaissent souvent mal les solutions qui leur permettront d'accomplir leur transformation numérique.

M. Alain Assouline. Il nous faut veiller à ne pas alourdir le poids des contraintes procédurales qui pèsent sur les entreprises. Souvent, la question de la sécurité a constitué un frein à l'innovation et à l'agilité. Or, je demeure convaincu qu'une prompte réactivité apporte la meilleure garantie de sécurité. Les forteresses ne résistent guère, particulièrement dans ce domaine.

Je soulignerai que le retard que nous enregistrons ne provient pas tant d'une insuffisance de l'investissement public. Il tient d'abord à la manière dont les projets ont été conduits. Ils n'ont pas assez pris en compte la question de la relation à l'utilisateur. À l'inverse, les GAFA assoient leur force sur une approche grand public. La nôtre privilégie trop la relation *B to B*, elle considère trop peu l'utilisateur final.

M. Alain Conrard. La transformation numérique implique certes de nouveaux usages dans l'entreprise ; elle les promeut surtout au niveau de l'individu. À la vérité, elle touche dans leur quotidien toutes les strates de la société.

À la suite de MM. Poyau et Rouri, je reconnais que nous devrions peut-être raisonner plus selon une logique de sensibilisation et d'acculturation. Obtenir que chaque individu prenne mieux en compte la nécessité de la transformation numérique favorisera ensuite la conduite de cette transformation au niveau entrepreneurial. Il me semble qu'orienter d'emblée et uniquement nos efforts à l'endroit des entreprises constituerait une erreur.

Nous le constatons à l'heure de procéder à une campagne de vaccination de grande ampleur. Nos autorités se trouvent dans l'obligation de doubler les plateformes d'inscription en ligne de traditionnels centres d'appels téléphoniques. Considérons donc les changements qui s'opèrent à l'aune de la population européenne dans son ensemble.

M. Laurent Giovachini. Ne nous accablons tout de même pas. En France, nous constatons que de nombreux services en ligne de nos administrations fonctionnent parfaitement bien. À titre d'exemple, dans le domaine des impôts, l'interface proposée, de conception purement nationale, s'avère particulièrement efficace à l'égard de toutes les catégories de citoyens. Sans doute, en matière de vaccin, l'absence d'anticipation joue-t-elle défavorablement et le ministère de la santé ne se révèle peut-être pas la plus en pointe de nos institutions sur les sujets qui nous intéressent.

M. Alain Assouline. Pour autant, l'État recrute 4 000 conseillers numériques, afin d'accompagner la population française dans l'utilisation de ses services en ligne.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur un dernier point. La France compte à ce jour un secrétariat d'État, mais pas de ministère de plein exercice, dédié au numérique. Nous relevons l'absence de véritable transversalité sur les questions qui relèvent de ce domaine. La précédente table ronde nous a appris que la direction interministérielle du numérique (DINUM) n'a nullement centralisé les demandes au moment où il a fallu répondre aux conséquences de la crise sanitaire sur les modalités d'organisation du travail et pourvoir nos fonctionnaires de réseaux privés virtuels (*virtual private networks*, VPN).

Les intervenants de cette première table ronde ont prôné un ministère du numérique à part entière. Respectant les spécificités de chaque secteur ministériel, il n'en effectuerait pas moins un travail transversal sur les enjeux du numérique. Que pensez-vous de cette proposition ?

M. Sylvain Rouri. Mon observation personnelle confirme, dans la situation d'urgence que nous avons vécue, une forme inquiétante de désorganisation, avec la sollicitation ministère par ministère des entreprises du numérique. L'absence de préparation, de schéma directeur et de coordination était flagrante. Notre discussion sur l'intrication des enjeux du numérique entre monde professionnel et grand public, entre entreprises, particuliers et citoyens, sur le fait qu'ils pénètrent tous les niveaux de la société, montre le sens qu'il y aurait à les embrasser de façon transversale, avec un ministère qui se consacrerait à ce travail.

J'ajoute que, dans la résolution des problèmes qui se posent, les organisations, les procédures et les outils ne constituent que des moyens. Il importe qu'en aval, la gouvernance et l'exécution suivent.

Lors du déclenchement de la crise sanitaire, l'une des principales faiblesses dans la réaction numérique a tenu à l'absence de gouvernance. L'écart s'est révélé trop important entre les annonces et directives du Gouvernement d'une part, leur appropriation et mise en œuvre d'autre part.

Installer un nouveau ministère ne prendra de sens que pour autant qu'il dispose véritablement des moyens d'agir. Il risque de se heurter au repli d'institutions qui se sont efforcés d'engager, chacune de son côté, leur propre transformation numérique. À ce jour, cette dispersion de l'effort national explique le peu de consistance de la commande publique et une certaine tendance à recourir à des solutions étrangères qui présentent l'avantage de la facilité.

M. Alain Assouline. Lors de sa mise en place au début du mandat de l'actuel Président de la République, le secrétariat d'État chargé du numérique a été rattaché au Premier ministre, sans disposer d'administration spécifique. Depuis, il est revenu dans le périmètre du ministère de l'économie, des finances et de la relance. Ses compétences y sont disputées. Il ne traite par exemple pas de la transformation numérique des TPE-PME. Le ministre délégué aux petites et moyennes entreprises s'en charge.

La CPME soutient la création d'un ministère de plein exercice, qui dispose de moyens réels, avec une administration dédiée, afin de conduire une action transversale sur les sujets inhérents au numérique.

M. Christian Poyau. J'aimerais saluer le travail de terrain, particulièrement concret, que conduit M. Cédric O, l'actuel secrétaire d'État chargé de la transition numérique et des communications électroniques.

Certes, au sein de nos institutions, il demeure possible de parfaire l'organisation du pilotage des questions numériques, mais la remarque vaut aussi pour toutes les entreprises de quelque envergure. Dans ces dernières, nous remarquons une même hésitation quant à l'attribution de ce pilotage à l'une des directions qui les structurent. Le numérique y revient-il à la direction financière, à la direction opérationnelle, à celle du marketing, ou encore à celle en charge des systèmes d'information ?

Cependant, l'attitude des responsables politiques en poste me surprend. Bien qu'ils s'avèrent, au plus haut niveau de l'État, parfaitement conscients des enjeux du numérique, et qu'au surplus ils l'affichent dans leurs discours, ils ne donnent à ces enjeux qu'une médiocre traduction dans les textes.

M. Philippe Latombe, rapporteur. Souhaitez-vous évoquer d'autres aspects du sujet qui nous rassemble ?

M. Sylvain Rouri. Je rappellerai l'importance de soutenir les *startups*. Elles quittent en nombre trop élevé notre territoire. La raison en tient au fait que les géants américains et chinois du numérique leur accordent des bons d'utilisation gratuits (*vouchers*) des infrastructures de leurs plateformes, ce qui les enferme techniquement. Elles ne parviennent ensuite que difficilement à s'affranchir de ces infrastructures et à s'émanciper.

M. Alain Assouline. J'ajouterai une brève observation au sujet de la formation de nos talents aux métiers du numérique. Une compétition mondiale s'est engagée. Notre capacité à former de nouveaux et nombreux talents dans les différents domaines du numérique jouera vraisemblablement un rôle fondamental dans la promotion de notre souveraineté numérique.

M. Laurent Giovachini. À condition, toutefois, que ces talents que nous formons dans nos écoles et universités rejoignent effectivement les entreprises françaises et européennes. Tel n'est pas toujours le cas. Nous formons sans doute plus de talents que nous n'en employons. Des filières du numérique connaissent des situations de pénurie de compétences. Si elles veulent les attirer et retenir, nos entreprises doivent demeurer attractives. Nous nous confrontons à une situation que nous avons rencontrée quelques décennies en arrière dans le secteur financier, quand nos diplômés choisissaient volontiers de partir pour des banques étrangères.

M. Alain Assouline. Vous avez raison. Il ne suffit pas de former nos talents. Encore faut-il nous donner les moyens de les garder.

M. Christian Poyau. Soulignons de plus combien le développement des outils numériques dépend de la qualité de nos infrastructures. Je pense en particulier aux réseaux de télécommunication, à la fibre et à la 5G. Nous devons continuer à avancer sur ces sujets et je regrette certains débats actuels, notamment au sein de collectivités territoriales, qui visent à réfréner notre marche.

M. Alain Conrard. En dernier lieu, j'appuierai sur ce que nous manquons cruellement de formations et d'actions d'information auprès des publics les plus jeunes, spécialement ceux des collèges et lycées, sur les enjeux majeurs dont nous avons traité. Au sens large du terme, l'innovation gagnerait à intégrer les programmes de l'enseignement secondaire.

M. Philippe Latombe, rapporteur. Vous n'êtes pas les seuls à avoir soulevé la question de la formation. Elle concerne notre système éducatif dans son ensemble, de l'école à l'enseignement supérieur et à l'alternance. Elle conduit à nous interroger sur la manière de conserver ensuite nos talents. La mission d'information sera vraisemblablement amenée à l'approfondir dans la suite de ses travaux.

Je vous remercie pour le temps que vous nous avez consacré.

Audition de M. Edward Jossa, président de l'Union des groupements d'achats publics (UGAP) et de Mme Pierrette Vidal, directrice commerciale secteur public,et M. Michel Ferrand, directeur avant-vente de Specialist Computer Company France (SCC France)
(21 janvier 2021)

Présidence de M. Philippe Latombe, Rapporteur.

M. Philippe Latombe, rapporteur. Bonjour à tous. Notre mission d'information poursuit ses travaux avec deux auditions consacrées à la souveraineté numérique et à la commande publique. Nous auditionnons l'Union des groupements d'achats publics (UGAP) et Specialist Computer Company France (SCC France), un acteur privé spécialiste de la transformation digitale des organisations et fournisseur de l'UGAP.

Notre objectif est d'échanger avec vous sur la façon dont la commande publique peut être mise au service de la transformation numérique de nos administrations et de la construction d'une forme de souveraineté numérique nationale ou européenne.

Nous recevons aujourd'hui M. Edward Jossa, président-directeur général de l'UGAP, Mme Pierrette Vidal, directrice commerciale secteur public, et M. Michel Ferrand, directeur avant-vente, au sein de SCC France.

J'aimerais d'abord que vous nous indiquiez ce que recouvre, selon vous, la notion de souveraineté numérique. Ce concept fait l'objet d'une attention croissante de la part des pouvoirs publics, notamment depuis la crise sanitaire. Nous avons, au cours de nos auditions, eu l'occasion de recueillir plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. Je suis intéressé par le regard que vous portez sur ce concept et la façon dont il peut, selon vous, se traduire concrètement au sein de l'action publique.

En second lieu, je souhaiterais échanger avec vous sur le contenu de la commande publique française et ses liens avec la promotion de notre souveraineté numérique. J'aimerais notamment savoir si les acteurs publics privilégient ou non, lorsque cela est possible, l'acquisition de matériels, de logiciels, de services numériques français ou européens. Je suis intéressé à connaître sur ce point votre analyse des forces et faiblesses de l'offre numérique française et européenne, et la façon de remédier à nos éventuelles carences.

Enfin, j'aimerais vous interroger sur la transformation numérique des acteurs publics. L'UGAP et SCC France participent à ce processus d'ampleur, en fournissant du matériel, des logiciels et des services numériques aux administrations. Je souhaiterais que vous nous indiquiez quelles sont les pratiques et les attentes des acteurs publics dans ce domaine, mais aussi le cas échéant, leurs difficultés. Cette question fait le lien avec le sujet de la cybersécurité, et le besoin de développer au sein de la sphère publique une véritable culture de la sécurité numérique.

Je vous cède maintenant la parole pour un propos liminaire d'environ dix minutes chacun, puis nous engagerons le dialogue sur la base des éléments que vous nous aurez apportés.

Mme Pierrette Vidal, directrice commerciale secteur public, Specialist Computer Company (SCC) France. Fondé en 1975 par Sir Peter Rigby, SCC est une entreprise familiale, aujourd'hui devenue le premier groupe privé européen. Le groupe SCC est classé

sixième du top 10 des entreprises de services du numérique (ESN) en 2020. En Europe, nous intervenons en Angleterre, en France, en Espagne et en Roumanie et réunissons environ 5 000 collaborateurs. Nous avons réalisé l'année dernière un chiffre d'affaires de 2,7 milliards d'euros. En France, notre chiffre d'affaire s'élevait à 1,7 milliard d'euros l'année dernière – le secteur public représentant plus de 55% de ce montant. Nous employons plus de 3 000 collaborateurs en France. Notre présence en France s'étend sur tout le territoire national par 23 agences commerciales, 55 points techniques, un solution-center, quatre centres de services et un grand centre logistique situé à Lieusaint pour tout ce qui a trait au stockage et à l'intégration des matériels déployés.

SCC est un intégrateur de solutions technologiques. Nous accompagnons tous nos clients – privés, publics ou entreprises de taille intermédiaire (ETI) – dans leur transformation numérique. Nos offres associent solutions technologiques et services associés. Nous intervenons dans différents domaines, au premier rang desquels la modernisation des infrastructures et l'évolution vers le *cloud (*privé, public ou hybride) de façon sécurisée, prenant en compte le développement des usages et l'expérience des utilisateurs.

Nous intervenons tout au long du cycle de vie d'un projet, à commencer par le conseil, puis la mise en œuvre, le stockage, le déploiement, l'aide aux utilisateurs (services desk et proximité). Nous gérons également la fin de vie de tous nos produits à travers une filiale spécialisée. Tout ceci est encapsulé avec des offres de financement pour nos clients, si besoin. Pour que nos clients puissent disposer d'une visibilité globale de leurs projets, nous avons mis en place une suite outillée permettant le suivi et l'analyse.

Je vous présenterai les réalisations de 2020 et l'actualité 2021 de SCC. Nous avons connu un franc succès en matière d'accompagnement de services. Tous nos investissements ont été réalisés pour accompagner nos clients français et européens sur des centres de production français. Pour preuve, la réussite de notre centre de services Recyclea : il s'agit d'une entreprise adaptée spécialisée dans la fin de vie des équipements. Nous y employons aujourd'hui plus de 70% de personnes en situation de handicap, à Montluçon. Nous continuons également le développement d'Altimance, un centre de services aux utilisateurs ouvert en 2016. Situé à Valenciennes, il emploie plus de 300 collaborateurs, pour la plupart des jeunes diplômés et des jeunes en réinsertion sociale. Il nous a valu le prix Choose France pour la cohésion et la solidarité.

En 2021, SCC ouvrira un nouveau centre de services à Montluçon, Altimancea. Nous continuerons nos développements, à savoir : la recherche de partenaires innovants dans les domaines du *cloud*, de l'hybridation, de l'internet des objets (IdO ou *IOT*), ainsi que la modernisation de nos propres infrastructures et l'obtention de la certification ISO 27001 pour notre direction des systèmes d'information (DSI), qui constitue le pilier de la transformation numérique de nos activités.

M. Edward Jossa, président-directeur général de l'Union des groupements d'achats publics (UGAP). L'UGAP est une centrale d'achat au sens du droit communautaire et national. L'UGAP est responsable de la publication des appels d'offres, et, par conséquent, les clients publics de l'UGAP sont dispensés de mener ces procédures. Ce modèle, qui se généralise, vaut pour l'UGAP comme pour toutes les grandes centrales d'achats européennes. Il se caractérise avant tout par la dispense de procédures dont bénéficient les administrations qui ont recours aux services de l'UGAP.

La deuxième caractéristique principale de l'UGAP est qu'elle constitue une centrale d'achat généraliste. Elle est ainsi la principale centrale d'achat public généraliste en France. Nous intervenons dans absolument tous les domaines, sauf : le militaire, qui est régi par une

réglementation particulière, le bâtiment et les travaux publics, qui sont eux aussi soumis à des règles particulières liées à la relation avec la maîtrise d'ouvrage, l'alimentaire pour des raisons historiques, et enfin le médicament, car la commercialisation du médicament est soumise à une législation spécifique. L'UGAP intervient ainsi actuellement dans l'achat des tests antigéniques mais non des vaccins.

Dans toutes ses activités, l'UGAP travaille avec 700 fournisseurs de premier rang. En vérité, la notion de fournisseurs de premier rang ne correspond pas à la réalité de l'activité, car les fournisseurs de second rang sont bien plus nombreux.

La clientèle de l'UGAP se compose de 22 000 entités. Parmi elles comptent l'État, les collectivités territoriales et les collectivités hospitalières. L'UGAP traite en réalité avec l'ensemble des entités soumises à l'application du code de la commande publique en France. Ce champ d'application peut également inclure des structures privées, si celles-ci sont majoritairement subventionnées ou si elles interviennent sur des missions de service public. Le champ d'intervention de l'UGAP est ainsi exactement le champ d'application du code de la commande publique. Aujourd'hui, 43% des ventes concernent l'État et les établissements publics, 31% les collectivités territoriales et 26% les autres entités (principalement le secteur hospitalier).

La troisième caractéristique principale de l'UGAP est qu'elle intervient en mode grossiste. Cela la distingue de la quasi-totalité des centrales d'achats en France et en Europe. Dans la plupart des cas, les centrales d'achats regroupent des acheteurs face à un marché collectif, obtiennent ainsi une meilleure performance économique, puis chaque acteur mobilise le marché. Le modèle de l'UGAP est différent : juridiquement, l'UGAP achète aux fournisseurs puis revend. Elle porte donc totalement l'action de l'achat et de la revente. Pour une centrale d'achat, cela s'appelle intervenir en mode grossiste.

La quatrième caractéristique de l'UGAP, qui est étroitement liée au fait qu'elle travaille en mode grossiste, est qu'elle intervient – c'est là encore une particularité de la France – sous la forme d'un établissement public industriel et commercial (EPIC). Puisque l'UGAP achète et revend, elle peut se financer par la constitution d'une marge. Le choix de la France, opéré dans les années 1960, a été de privilégier le mode grossiste. Historiquement, l'UGAP était une structure d'approvisionnement et de vente aux écoles, qui relèvent de la compétence communale. Ce modèle d'achat et de revente a pour conséquence que l'EPIC ne reçoit pas de subvention de l'État et porte la responsabilité de ses marchés. La structure doit donc gérer ses marchés de manière à obtenir des ressources à l'équilibre. L'établissement est d'ailleurs soumis à l'impôt sur les sociétés et génère un bénéfice, qui revient à l'État puisque l'établissement est à 100% public. La structure est donc un réel EPIC, bien qu'elle intervienne sur des matières proprement régaliennes.

La stratégie de l'établissement se fonde sur trois éléments. Tout d'abord, une évolution maîtrisée de l'offre : nous ne pouvons pas intervenir dans tous les domaines, et nous devons choisir les sujets prioritaires pour les entités qui font appel à l'UGAP. Cela est d'autant plus vrai que, sauf en cas d'instruction ministérielle, la règle est que les clients publics ont le choix de recourir ou non à l'UGAP. Cet élément est fondamental. L'UGAP doit donc acheter les produits qui se vendent. Cela est très important. L'UGAP est responsable économiquement de la performance de ses achats.

La valeur ajoutée du modèle de l'UGAP se situe dans l'exécution : le modèle de l'exécution a le mérite de rendre des services accrus à la fois aux fournisseurs et aux clients. Aux fournisseurs, car en vendant à l'UGAP, les fournisseurs sont en rapport avec un seul point de vente, et non avec la multitude des interlocuteurs du secteur public ; cela facilite

énormément la relation commerciale ainsi que la facturation. L'UGAP met d'ailleurs un point d'honneur à payer à date, à 30 jours, ce qui constitue une sécurité et une garantie de trésorerie très appréciables pour les entreprises – et peut-être d'autant plus pour les PME avec lesquelles nous travaillons directement. Cela nous a permis de jouer un rôle très positif pendant la crise : nous avons versé 100 millions d'euros de paiements anticipés aux entreprises et avons donc représenté un soutien aux entreprises pendant cette période très difficile.

Voilà les éléments principaux de présentation de l'UGAP. Souhaitez-vous que je poursuive mon propos par l'analyse des enjeux propres à la souveraineté numérique ?

M. Philippe Latombe, rapporteur. Absolument, cela me paraît logique.

M. Edward Jossa. S'agissant de la définition de la souveraineté numérique, d'autres personnes sont bien plus compétentes que moi pour s'exprimer à ce sujet. Il me semble qu'il existe, dans la souveraineté numérique, certains sujets indissociables de la souveraineté économique générale, et des sujets plus spécifiques au numérique.

Les enjeux indissociables de la souveraineté économique générale sont la nationalité des entreprises et la nationalité des produits. Ces deux éléments peuvent très bien ne pas correspondre. La nationalité des entreprises est un enjeu de pouvoir et un levier important. Quand le potentiel rachat de Carrefour a été envisagé, nous avons bien vu à quel point la nationalité de l'entreprise constituait un enjeu de pouvoir. La nationalité des produits est quant à elle un enjeu purement économique. En tant que centrale d'achat, l'UGAP doit gérer des complexités propres à ce sujet : même si elle traite avec des entreprises étrangères, l'UGAP travaille toujours avec des filiales de droit français et implantées en France. Cela montre que la notion de nationalité économique n'est pas si simple que cela à cerner.

Les enjeux propres au numérique sont tout d'abord la localisation de la donnée et la maîtrise de la donnée. Cela recouvre deux catégories différentes de données.

Cela concerne tout d'abord les données produites lors de transactions entre une entreprise et des particuliers. Cela est le modèle des GAFA, qui disposent de données produites dans le cadre de la relation avec l'entreprise : lorsque vous achetez sur Amazon ou que vous surfez sur Facebook, par exemple. La donnée est donc propriété de l'entreprise. Le domaine de la protection des données personnelles est mobilisé pour répondre à ce sujet, c'est pourquoi le RGPD revêt une importance cruciale en la matière ; néanmoins, les réponses apportées à ce sujet se sont traduites concrètement par la multiplication des demandes de consentement adressées aux particuliers. Les particuliers les accordent de manière quasiment automatique désormais. Les vrais enjeux soulevés par ce sujet sont davantage la concurrence et la concentration de quantités de données considérables, qui constituent le propre du modèle adopté par les GAFA.

La deuxième catégorie de données recouvre les données à protéger et à conserver sur le territoire. Il s'agit des données de l'État ou des entreprises, liées à la sécurité par exemple, et qui transitent par des systèmes d'exploitation ou des serveurs qui sont sur le *cloud*. L'enjeu n'est donc pas la production de la donnée mais la protection de la donnée existante.

Il convient de bien distinguer ces deux enjeux, qui se traitent par des solutions différentes. Il me semble que la première catégorie de données peut être traitée par des solutions relevant du droit économique et du droit de la concurrence, afin d'éviter les concentrations et les abus de position dominante quand ceux-ci se font au profit d'acteurs extérieurs à la France. Le deuxième sujet se traite par des règles de protection, des solutions de souveraineté permettant notamment le *cloud* souverain.

Je ne pense pas néanmoins que les enjeux de souveraineté numérique se limitent à ces enjeux liés proprement à la donnée. Je rappellerai par exemple l'extraordinaire concentration des systèmes d'exploitation : en téléphonie mobile, elle repose sur Android ou Apple ; dans les ordinateurs, sur Windows ; nous constatons la même tendance archi-monopolistique dans les télécommunications, avec une concentration d'entreprises étrangères dans les solutions que nous utilisons. Nous communiquons aujourd'hui via Zoom. Cela témoigne des enjeux d'une concentration d'éléments absolument stratégiques dans le domaine des télécommunications. Ce phénomène est accru par les fortes interactions existant entre les différents éléments dans le secteur informatique : entre le software et le hardware, ou entre les différents logiciels entre eux, par exemple. Cela questionne les interdépendances et la capacité à faire de manière autonome. Je pense donc que les enjeux généraux de la souveraineté numérique nécessitent une vision globale des interactions existantes entre tous ces sujets.

Je souhaiterais maintenant évoquer la manière dont ces enjeux s'articulent avec la commande publique, et montrer comment l'UGAP applique le code de la commande publique dans ce contexte très particulier. Pour comprendre plus concrètement notre sujet, j'évoquerai chacun des segments de l'informatique : les matériels, les logiciels, puis les prestations informatiques.

S'agissant des matériels au sens large, la France est quasi absente de la micro-informatique et des serveurs. Ce marché est aujourd'hui complètement dominé par HP, Lenovo et Dell. L'UGAP ne passe même plus de marchés directs de matériels, mais a recours à des distributeurs. En 2020, l'activité de l'UGAP représentait 734 millions d'euros sur ce segment, dont 500 millions d'euros étaient partagés entre les trois grands distributeurs avec lesquels l'UGAP travaille (SCC, Computer Center et Econocom). La pratique des grandes entreprises comme HP et Lenovo n'est pas de vendre en direct mais de vendre par des distributeurs. En la matière, le marché impose donc bien son modèle à la commande publique. Seuls deux secteurs échappent à ce principe de passage obligé par des revendeurs : il s'agit des photocopies et télécopies, pour lesquels les grands acteurs répondent en direct (Toshiba pour les photocopieurs, Xerox pour les copieurs). Ils forment donc des marchés plus classiques du point de vue de la commande publique. Je citerai à ce sujet quelques exceptions d'entreprises françaises : la société Nomios intervient en matière de cybersécurité. Le marché spécifique conclu avec cette entreprise se justifie par le fait que leur produit est hybride et mêle matériel, logiciel et prestation intellectuelle. Elle constitue une exception à ce principe sur le segment des matériels.

S'agissant du segment des logiciels, la situation est encore plus compliquée. Certains logiciels, dont tout le monde a besoin, sont extrêmement concentrés et imposent leur loi au marché. Dans le même temps, il existe une foultitude de créateurs de logiciels, dont énormément d'entreprises françaises. La difficulté, au regard du code de la commande publique, est la comparabilité. Le code de la commande publique est destiné à faire respecter les règles de la concurrence, et la concurrence repose sur la comparabilité des produits. Or, le secteur des logiciels est extrêmement instable et la valeur des produits est extraordinairement difficile à déterminer. Qu'il s'agisse de grands ou de petits créateurs de logiciels, les prix des produits sont fixés de manière tout à fait arbitraire selon les clients, selon les quantités achetées ou selon l'articulation du logiciel avec les services associés. Tous ces éléments forment donc un marché très difficile à cerner. Le modèle économique a conduit à une claire prédominance des distributeurs, qui constituent quasiment la seule solution pour acheter un logiciel. L'UGAP a conclu deux marchés spécifiques pour des logiciels indispensables, dont le modèle de vente ne passe que par des revendeurs : il s'agit d'Oracle et du matériel Microsoft. Pour ces marchés, l'UGAP met en concurrence les revendeurs.

Cela me permet de répondre à l'une de vos interrogations sur le projet Health Data Hub. Le ministère a mobilisé notre marché dédié à l'achat d'équipement Microsoft. Nous avons pour cela mis en concurrence les différents revendeurs, et c'est de cette manière que s'est faite l'attribution du marché. L'UGAP n'intervient pas en la matière : le ministère achète le logiciel et l'UGAP ne sait pas à quelles fins l'État mobilise les logiciels achetés ; il ne relève d'ailleurs pas de sa mission de le savoir, mais seulement de vérifier que les logiciels sont achetés au prix et aux conditions contractuelles du marché.

Dans le domaine des logiciels, nous travaillons quasiment exclusivement soit sur ces deux marchés dédiés, soit sur un marché inventé par l'UGAP et repris depuis par les autres centrales d'achats : le marché multi-éditeurs. Nous mettons en concurrence des bibliothécaires de logiciels. Le marché multi-éditeurs est d'ailleurs le marché le plus important de l'UGAP : il regroupe 3 000 éditeurs. La valeur du revendeur réside évidemment dans le prix qu'il nous offre pour ses produits, mais également dans les services associés. Pour gérer un tel nombre de logiciels, il faut disposer d'une vraie plateforme performante, qui permet de repérer les caractéristiques des logiciels et de les mettre en comparaison. La valeur réside dans la prestation qui permet la fluidité de la consommation.

M. Philippe Latombe, rapporteur. Je me permets une incise car vous avez évoqué un dossier qui nous intéresse en particulier. Nous auditionnerons dans quelques semaines le Health Data Hub et d'autres services. Le ministère vous a-t-il demandé d'acheter Microsoft pour le Health Data Hub ?

M. Edward Jossa. Nous avons reçu une commande. Nous disposons d'un marché Microsoft. Oui, nous avons reçu une commande du ministère pour intervenir sur notre marché Microsoft.

M. Philippe Latombe, rapporteur. Cela vous arrive-t-il souvent de recevoir ce genre de commande ? Dans ce cas précis, je comprends que vous avez été exécutant d'une décision prise par l'État.

M. Edward Jossa. L'UGAP fonctionne sur commande. Nous avons un marché Microsoft – nous ne traitons d'ailleurs pas en direct avec Microsoft, mais avec un revendeur, en l'occurrence SCC, qui est le titulaire de notre marché Microsoft. Notre rôle est de vendre ce qui nous est acheté, aussi simplement que cela.

M. Philippe Latombe, rapporteur. Merci. Je souhaitais comprendre très clairement vos propos.

M. Edward Jossa. Nous vérifions néanmoins une convenance des prix. Nous essayons également de protéger les clients contre les achats trop nombreux de licences : parfois, les règles propres à chaque éditeur causent des négociations compliquées sur le nombre de licences autorisées. Nous ne jouons en revanche aucun rôle dans les décisions prises par les acteurs publics de recourir à telle ou telle solution. La plupart du temps d'ailleurs, si vous disposez d'un système central sur SAP, il est extrêmement coûteux d'en changer. Il existe donc des pratiques extrêmement contraignantes dans ce domaine. En tant que telle, l'UGAP ne peut que vérifier la commande auprès d'un distributeur.

J'en terminerai au sujet des logiciels. Nous avons réalisé en 2020 594 millions d'euros de ventes de prestations. Le principal acteur en est SCC, qui est majoritaire dans ce domaine car titulaire du marché multi-éditeurs. Le marché multi-éditeurs est un des principaux outils par lequel il serait possible de faire émerger des entreprises françaises de logiciels dans la commande publique. Nous cherchons à mobiliser ce marché pour répondre à des objectifs de

politique publique. Ainsi, notre cellule innovation repère des PME ; si les solutions qu'elles proposent nous paraissent bonnes et semblent correspondre aux besoins des collectivités locales, alors nous discutons, notamment avec SCC, de leur intégration dans le marché multi-éditeurs. C'est de cette manière que nous avons obtenu le logiciel Doctolib, aujourd'hui référencé dans le marché multi-éditeurs. C'est également le cas de Talentsoft, une très belle entreprise française. Le marché multi-éditeurs est donc un vecteur important de politique publique.

M. Éric Bothorel. Cette architecture d'approvisionnement de produits, dont l'UGAP constitue une interface privilégiée pour la commande publique, n'a-t-elle pas évolué pour vendre davantage des services que des produits ? J'entends ce matin des propos qui me ramènent vingt ans en arrière, à l'époque où je travaillais chez Infopoint. Le marché du logiciel a longtemps été considéré comme un marché de produits. Nous pouvons imaginer, s'agissant du Health Data Hub, que par convenance et par facilité, le ministère a choisi d'acheter des briques Microsoft. Mais lorsque l'on achète du software, en mode SaaS ou autre, cela revient à acheter une prestation de services. Nous évoluons aujourd'hui vers un système où les logiciels sont facturés à l'heure, par exemple – ce modèle n'existait pas il y a dix ans. À l'époque, notre consommation de logiciels reposait sur l'acquisition d'une licence qui permettait d'utiliser le produit sans en être propriétaire ; cela n'est plus le cas aujourd'hui. Le modèle d'approvisionnement en place aujourd'hui correspond-t-il toujours à la façon dont nous consommons le logiciel ? Je ne parle ici que des offres sur étagère. Le marché du logiciel a fortement évolué. Les référencements à l'UGAP sont-ils encore adaptés, alors que le marché évolue en permanence ?

M. Edward Jossa. Nous nous posons cette question tous les jours. Tout le défi pour l'UGAP est de s'adapter à la réalité du marché. En la matière, nous avons distingué les logiciels et les services.

Je commencerai par les marchés de service. En sus des 594 millions d'euros issus de la vente des logiciels, nous vendons chaque année pour 350 millions d'euros de services. Ce secteur est différent de celui des logiciels : il regroupe certaines entreprises françaises très performantes, comme Capgemini et Atos. C'est le seul secteur dans lequel existent quelques géants français. Il faut savoir mobiliser nos atouts dans la compétition internationale dans ce domaine.

Revenant à votre question, la valeur de logiciels s'entend par l'association étroite entre les logiciels et les services. C'est la raison pour laquelle nos marchés de service utilitaires prévoient des services associés aux logiciels dans la prestation. Nous nommons le marché « marché de logiciels », mais la construction contractuelle de ce marché est faite de sorte à intégrer une part de services. Cela est parfois d'ailleurs très compliqué en termes de facturation pour les clients publics. Les règles de la comptabilité publique ne sont pas simples à ce sujet. Il y a donc une part de services dans les marchés de logiciels.

Le marché du *cloud* est encore différent. Nous sommes passés par un intégrateur, en l'occurrence Capgemini qui a remporté le marché et qui propose plusieurs solutions. Nous avons fait le choix de faire appel à différents fournisseurs de *cloud* : parmi eux, les fournisseurs incontournables, comme Amazon Web Services (AWS) ou Azur de Microsoft ; mais aussi Outscale, OVH, Scaleway, Oracle. Notre marché de *cloud* regroupe plusieurs fournisseurs. Il revient au client de choisir le fournisseur auquel il souhaite recourir et il doit justifier son choix. Notre marché prévoit ainsi un module qui explique les raisons d'intérêt général qui peuvent présider au choix de nos clients. De plus, nous portons une grande attention au dispositif de labellisation. La norme SecNumCloud est importante en termes de souveraineté numérique. Notre fournisseur OVH dispose de la norme SecNumCloud. Si le client public

requiert, pour ses données, un fournisseur titulaire de la norme SecNumCloud, il peut trouver satisfaction dans ce marché.

Il existe également un enjeu d'articulation de la prestation *cloud* pure avec les prestations de conseil. Cette question est particulièrement sensible pour les collectivités territoriales, qui ne sont pas toujours dotées de directions des services informatiques (DSI) aussi puissantes que peuvent l'être celles des entreprises ou de l'État. Nous lançons en ce moment un marché de conseil, qui sera publié dans quelques semaines.

M. Philippe Latombe, rapporteur. La fourniture des services de conseil est-elle préalable au *cloud* ? Comment est-elle séquencée ? Si la société chargée d'effectuer la mission de conseil propose ensuite systématiquement la solution d'un seul fournisseur de *cloud*, la commande est orientée.

M. Edward Jossa. C'est justement pour assurer une forme d'indépendance du conseil et du *cloud* qu'il nous a été demandé de procéder à la publication de deux marchés bien distincts : un premier pour les prestations de *cloud* brutes, et un second pour les prestations de conseil. Nous effectuerons une forme de surveillance de la neutralité des acteurs du conseil vis-à-vis des acteurs du *cloud*.

M. Éric Bothorel. Je propose de recourir à un cas concret. Admettons qu'une petite agglomération de 20 000 habitants dispose d'une salle informatique vieillissante. Elle souhaite migrer son système d'information (SI) dans le *cloud*. Elle va devoir recourir à la commande publique et donc se tourner vers l'UGAP. Quels sont les flux ? Qui interagit avec qui ? Comment les échanges se déroulent-ils ?

M. Edward Jossa. Nous disposons d'un réseau commercial dont les directions territoriales sont implantées dans tout le pays. Nos conseillers informatiques spécialisés orientent le client public vers la meilleure solution. Dans un premier temps, cela peut être de proposer au client public du conseil en stratégie informatique, en organisation, voire en cybersécurité. La première étape est donc de fournir des prestations de conseil. Ensuite, l'UGAP oriente la collectivité, en fonction de ses besoins, vers une solution purement logicielle ou bien vers une solution de *cloud*. Tout ceci doit permettre d'assurer la cohérence des équipements, matériels et prestations souhaités. Nous disposons d'une gamme complète de services. Il revient au conseiller informatique de l'UGAP d'orienter correctement le client vers les solutions dont il a besoin.

M. Éric Bothorel. Comment feriez-vous alors pour conseiller cette collectivité qui a besoin d'un hébergeur ? Sur quels critères décideriez-vous de l'orienter plutôt vers OVH ou vers AWS ?

M. Edward Jossa. La manière classique de travailler de l'UGAP recouvre les étapes suivantes : conseil, puis devis, puis commande. Sur un certain nombre de solutions, comme le marché multi-éditeurs ou le marché *cloud*, tout notre travail consiste à incorporer des outils d'aide à la décision dans notre dispositif de commande. Cet outil d'aide à la décision repose sur un système de questions et réponses : le client entre les données relatives à ses besoins et à sa commande. Capgemini, titulaire du marché, est responsable d'entretenir une application d'aide au choix qui permet d'objectiver les critères guidant la prise de décision. Cela permet d'éviter une forme d'arbitraire qui présente un risque pour l'UGAP tout comme pour le client public.

M. Philippe Latombe, rapporteur. Vous avez évoqué la labellisation SecNumCloud. Si l'ordonnateur vous donne ce critère, il oriente forcément les solutions proposées.

M. Edward Jossa. Évidemment, si l'on entre ce critère, le système va sortir une solution correspondante : Outscale ou OVH.

M. Philippe Latombe, rapporteur. En effet. La labellisation SecNumCloud fait-elle partie des critères qui vous sont régulièrement demandés par vos clients ?

M. Edward Jossa. Cela dépend des besoins. Certains services spécialisés de l'État nous demandent la labellisation SecNumCloud. En revanche, si le client a besoin d'un puissant outil de gestion de ses données de ressources humaines ou de transports en commun, je ne vois pas quelle justification pourrait présider au recours à la labellisation SecNumCloud.

M. Philippe Latombe, rapporteur. Je peux le comprendre. Ma question est la suivante : la labellisation SecNumCloud fait-elle partie des critères bien présents à l'esprit des ordonnateurs ? Dans le cas du Health Data Hub, l'État vous a demandé de recourir à Microsoft. Mais les données traitées étaient très particulières et par conséquent, l'on est en droit de se demander où elles allaient être hébergées. De la même manière, une polémique a émergé au sujet de l'hébergement des données du prêt garanti par l'État (PGE) sur AWS, alors qu'elles pourraient potentiellement constituer des données sensibles. Je constate qu'il faut encore construire l'appétence et l'éducation des ordonnateurs publics à la sécurité des données et donc au recours à ce label. Cela n'est pas une critique envers l'UGAP.

M. Edward Jossa. Je ne peux pas répondre à cette question. L'UGAP n'est pas une autorité de prescription. La logique de l'UGAP est de fournir ce qu'on lui demande. Il faut sans doute renforcer la pédagogie, certes. L'animation et la formation constantes, au-delà des directeurs informatiques et incluant les décideurs (les secrétaires généraux des ministères, par exemple), peuvent contribuer à la prise de conscience de ces enjeux.

M. Philippe Latombe, rapporteur. Il nous a été rapporté, au cours de précédentes auditions et notamment par des PME françaises, que les acheteurs publics poursuivaient majoritairement des motivations de facilité, de rapidité et de solidité des systèmes. L'éducation de générations d'acheteurs publics est donc centrée sur l'utilisation de solutions de type Microsoft ou AWS, car celles-ci sont simples d'utilisation.

M. Edward Jossa. Les ministères poursuivent certaines priorités absolues et doivent gérer des problématiques d'urgence, comme nous le constatons en ce moment. Je ne vois pas comment une administration, d'autant plus dans le contexte actuel de crise sanitaire, peut prendre le moindre risque en matière d'opérationnalité. Il s'agit bien là d'opérationnalité. La tentation normale de tout décideur public est de ne pas avoir recours à une solution innovante s'il est question d'intervenir sur une partie clé de son système d'information. Le client public, aujourd'hui, ne tolère même pas une journée de rupture de service.

M. Philippe Latombe, rapporteur. Je prends l'exemple d'une grande entreprise publique ou parapublique qui souhaite changer son système de messagerie. Elle fait le choix d'opter pour Microsoft 365. Cela suppose de recourir à Azur pour stocker les mails en *cloud*. Pourquoi utiliser ces solutions ? Pourquoi opter pour Microsoft 365 et Azur, et ne pas remplacer Azur par une autre solution ? Est-ce uniquement parce que ces solutions sont intégrées et que cela ne se négocie pas ? Serait-il au contraire possible de segmenter ces services ?

M. Edward Jossa. Ces choix dépendent de la stratégie de chaque client. Il faut interroger à ce sujet chaque ministère ainsi que la direction interministérielle du numérique (DINUM). Ces choix recouvrent des enjeux d'opérationnalité. Les grands opérateurs ont de tels moyens qu'ils ont toujours un temps d'avance ; et le client public recherche avant tout la

performance. À mon sens, le sujet se traite davantage par l'angle économique que par celui de la commande publique. Il faut soutenir les champions nationaux ; l'enjeu est davantage d'éviter que ceux-ci soient rachetés par des entreprises étrangères.

M. Éric Bothorel. Peut-on donc toujours dire, comme on le disait dans les années 1990, que l'UGAP est un catalogue ?

M. Edward Jossa. Oui, au fond du fond, en matière informatique, l'UGAP est un grand catalogue.

M. Éric Bothorel. Si elle est un catalogue, peut-on reconnaître que la capacité de l'UGAP et de ses conseillers informatiques à influencer les acteurs publics est très peu utilisée ? Le travail de qualification et de prise de décision est souvent fait en amont, par l'aide de conseils, de revendeurs, de distributeurs, d'intégrateurs. Il apparaît alors que la seule capacité de l'UGAP à influencer les choix de marché est la disponibilité ou non d'un produit à son catalogue.

Je reviendrai sur la question posée au sujet du Health Data Hub. Le client public avait fait le choix d'opter pour Microsoft, mais il aurait tout aussi bien pu acheter de l'AWS ou de l'OVH puisque ces solutions sont disponibles au catalogue. La capacité d'influence de l'UGAP à orienter vers une solution plutôt qu'une autre n'existe donc pas.

M. Edward Jossa. L'UGAP ne se positionne pas de telle manière à influencer. Elle n'a pas vocation à se substituer aux décideurs publics. Nous sommes une centrale d'achat et notre mission est celle d'un facilitateur. Les ministères ne souhaitent pas que l'UGAP interfère dans leurs décisions. L'UGAP peut exercer une forme de contrôle, mais seulement quand elle est expressément mandatée pour le faire, par exemple en matière de voitures – cela constitue l'exception plutôt que la règle. La mission de l'UGAP est de faire respecter les règles de la concurrence et d'appliquer le code de la commande publique. S'il faut faire évoluer les choses, cela doit se jouer par des prescriptions adressées aux décideurs ; cela n'est certainement pas notre rôle et nous ne le revendiquons pas.

M. Éric Bothorel. Mais votre capacité d'influence peut s'exercer au moment de la consultation pour constituer le catalogue. Il vous appartient, au moment des consultations en vue d'un futur référencement, de sélectionner les produits. C'est de cela que se nourrit le catalogue mis à disposition.

M. Edward Jossa. Pas tout à fait. En matière de véhicules par exemple, nous élaborons un catalogue général qui correspond à tout ce que nous pouvons vendre ; en revanche, nous avons établi un catalogue resserré pour l'État, car seule la vente de certains véhicules est autorisée. L'UGAP fait ce que le client lui demande de faire.

M. Éric Bothorel. Quelle est la valeur ajoutée de l'UGAP dans ce cas-là ? Est-ce seulement le référencement de produits qui ont été choisis en amont ?

M. Edward Jossa. La valeur ajoutée de l'UGAP est de sécuriser les procédures de mise en concurrence, d'appliquer correctement le code de la commande publique, de faire gagner du temps aux clients, de procéder à des économies. Cela est exactement la mission de toutes les centrales d'achats en Europe. L'UGAP n'a pas de spécificité à ce sujet. Nous sommes là pour obtenir de meilleurs prix et pour faciliter la commande.

En revanche, si l'État décide qu'une partie des applications des ministères doivent obligatoirement bénéficier de la labellisation SecNumCloud, et que nous avons instruction de ne vendre que des produits labellisés SecNumCloud, alors nous l'appliquerons.

M. Philippe Latombe, rapporteur. Je poserai une question complémentaire à SCC. Les fournisseurs, qu'il s'agisse de sociétés informatiques petites ou grandes, concèdent-ils parfois de tels efforts commerciaux que leurs prix deviennent beaucoup moins chers que les autres services référencés ? Par exemple, AWS propose à beaucoup de jeunes entreprises des vouchers pour utiliser ses services et les rendre captives de son marché. Les grands acteurs tels que Microsoft ou Amazon s'adonnent-ils à des pratiques commerciales qui les positionnent de façon plus favorable sur le marché que d'autres petites entreprises qui n'en ont pas la capacité ? Comment, dans votre mission, déterminez-vous les pratiques qui relèvent d'une politique commerciale agressive ?

M. Michel Ferrand, directeur avant-vente, SCC France. Nous avons participé au marché *cloud* de l'UGAP, il y a un an. Nous sommes arrivés en deuxième position derrière Capgemini, mais nous avons bien suivi le déroulement des négociations avec les fournisseurs de *cloud*. Nous étions en contact avec quatorze d'entre eux et nous avons bien étudié leurs politiques de vente. Oui, ils concèdent des efforts commerciaux, et probablement plus importants que s'ils vendaient leurs services en direct à une collectivité locale ou à une entreprise privée. A contrario, ils ont tous mis en place une politique de justesse. Amazon pratique l'engagement de dépense pour disposer d'une tarification plus agressive dès le départ. Ils n'ont en revanche pas pratiqué cela avec SCC : les prix pratiqués avec SCC étaient hors engagement de dépense, car le marché de l'UGAP ne garantit pas de volume – il s'agit d'un référencement sur catalogue. La matrice d'aide au choix est capitale et ne doit pas être influencée : si les acteurs procèdent à des engagements de dépense impliquant des réductions, la matrice est faussée. Dans le cadre de l'UGAP, l'ensemble des fournisseurs de *cloud* a joué le jeu et n'a pas pratiqué l'engagement de dépense.

Un ministère ou une collectivité qui cherche la labellisation SecNumCloud afin de bénéficier d'une garantie de sécurité dans la matrice de choix de l'UGAP se verra proposer les seuls acteurs français labellisés : OVH et Outscale. Cela constitue une vraie sécurité. Mais il ne relève pas de l'UGAP de forcer le choix du ministère. Les ministères sont dotés d'équipes informatiques très compétentes et ils procèdent à leurs achats en toute conscience. Le choix d'achat est en revanche plus difficile pour les collectivités territoriales, souvent moins informées sur le sujet. Se met alors en place le jeu de la vente, qui consiste à mettre en avant une solution grâce au réseau territorial de revendeurs.

M. Philippe Latombe, rapporteur. Les petites entreprises ont rapporté à notre mission d'information que l'accès à la commande publique leur était très difficile. Quels sont les critères qui permettent de procéder aux achats ? Nous ne doutons pas que vous procédiez aux achats dans le respect des règles françaises et communautaires. Je m'interroge néanmoins sur les biais existants et cherche à savoir s'il est possible d'objectiver le ressenti communiqué par les entreprises lors des précédentes auditions.

M. Michel Ferrand. L'UGAP, comme SCC, y sont très sensibles. Les ministères ont des équipes informatiques très compétentes, sur les choix desquelles il est difficile d'influer. L'influence est en revanche très facile à exercer sur les services d'une collectivité locale. La situation est compliquée car les bénéficiaires finaux souffrent d'un important manque de compétences sur ces sujets.

M. Philippe Latombe, rapporteur. Je vois les choses de manière différente. Je préfère justifier l'achat de solutions toutes faites et simples d'utilisation par l'ignorance technique des

clients. Le client qui sait exactement ce qu'il veut, en revanche, fait un choix d'achat en toute conscience. Cela repose la question du choix de Microsoft dans le cas du Health Data Hub. La décision prise en toute conscience par quelqu'un de très compétent devient alors gênante.

M. Michel Ferrand. Je citerai un autre exemple. Le marché multi-éditeurs propose aujourd'hui un outil de visioconférence 100% français nommé Tixeo. Pourtant, il n'est pas acheté. L'UGAP comme SCC proposent des solutions alternatives, et pourtant nous n'arrivons pas à les commercialiser de façon importante. Il y a bien une raison à cela, et cela n'est pas dû à de la mauvaise volonté.

M. Philippe Latombe, rapporteur. S'agit-il d'une question d'acculturation ?

M. Michel Ferrand. Je le pense, en effet.

M. Edward Jossa. Je souhaiterais expliquer plus en détails comment nous essayons de favoriser les PME dans le marché multi-éditeurs, qui constitue l'un des outils les plus puissants mis en place en France pour favoriser la vente de logiciels français. Nous avons d'abord mis en place un dispositif d'identification. Il repose sur une cellule dédiée de trois ou quatre personnes qui consacrent leur temps à étudier les propositions de logiciels reçues et à déterminer lesquelles sont pertinentes. Le travail d'identification est capital : il est nécessaire de faire le tri dans toutes les solutions qui nous sont proposées. Puis, nous étudions lesquelles d'entre elles sont pertinentes au regard des besoins du secteur public. Nous avons ainsi conclu des partenariats de recherche et d'innovation avec des collectivités territoriales, qui nous aident dans ce travail de qualification des solutions. Une fois la solution retenue, nous l'intégrons dans notre offre. La solution multi-éditeurs fait gagner un temps précieux à l'éditeur. Une fois la solution ajoutée au catalogue de l'UGAP, il est encore nécessaire de la faire connaître. Cela est peut-être le sujet sur lequel nous devons encore le plus travailler. Nous mettons en place un dispositif de conseil et d'assistance aux titulaires pour mieux faire à ce sujet. Nous avons été des accélérateurs de croissance colossaux pour certaines solutions ; il faut également que les entreprises puissent faire face à l'afflux croissant de demandes, potentiellement dans un temps très réduit. 50% des titulaires auprès de l'UGAP sont des PME ; toutes activités confondues, les PME représentent 20% du volume du chiffre d'affaires de l'UGAP. Elles sont principalement présentes dans le secteur du mobilier, du conseil et du logiciel.

M. Philippe Latombe, rapporteur. Certains outils de financement existent pour les titulaires de marchés. Ils permettent d'accompagner la montée en charge des PME.

Imaginons qu'une volonté politique forte émerge pour privilégier les solutions françaises et européennes : selon vous, quels éléments devraient être modifiés dans les pratiques comme dans la législation ? Nous avons évoqué la labellisation SecNumCloud. Existe-t-il d'autres leviers pour favoriser les solutions françaises et européennes ?

M. Edward Jossa. L'article L. 2153-1 du code de la commande publique prévoit le principe d'égalité de traitement des opérateurs économiques issus de l'Union européenne avec ceux issus d'États faisant partie de l'accord de marchés publics de l'Organisation mondiale du commerce (OMC). Le principe du code de la commande publique est l'égalité de traitement entre Européens et les nombreux non-Européens signataires de cet accord. À ma connaissance, cet accord n'inclut pas la Chine, mais inclut le Japon, la Corée du Sud et les États-Unis. La direction des affaires juridiques de Bercy ainsi que la direction générale des entreprises sont les acteurs les plus qualifiés pour évoquer ces sujets. Une réflexion est en cours vis-à-vis des pays non-membres de l'accord. Il est néanmoins difficile de prendre des mesures discriminatoires. L'application des règles du code de la commande publique est, en ce sens,

un élément stabilisateur. Nous essayons d'inclure, quand cela est possible, des clauses conformes au code de la commande publique qui permettent d'intervenir – cela est le cas, par exemple, dans le domaine des véhicules. Mais ces clauses doivent être proportionnées à l'enjeu. Nous essayons également de développer des clauses d'audit social. Nous disposons de clauses sociales internes à la France, et nous réfléchissons à des clauses sur la bonne application du droit du travail du pays d'origine. Dans un certain nombre de marchés, nous avons ajouté des clauses selon lesquelles le fournisseur doit apporter un audit de la conformité de ses pratiques par rapport au droit du travail. Cela est particulièrement important dans des secteurs comme le textile, mais d'autres sujets majeurs peuvent apparaître. Une prise de conscience collective émerge sur ces sujets.

Mme Pierrette Vidal. Certains clients ont des idées bien arrêtées sur les solutions qu'ils souhaitent acquérir. Cela n'est pas parce qu'ils souhaitent acheter AWS ou Microsoft, mais parce qu'ils disposent de personnels habitués et formés à travailler sur ces interfaces. Les ministères souffrent d'un manque de personnels et sous-traitent de plus en plus ; ils ont besoin d'être opérationnels rapidement.

À titre d'exemple, nous avons remporté l'année dernière le marché interministériel du stockage : nous avons pour cela proposé plusieurs solutions. À l'usage, nous constatons que 80% à 85% des personnes n'achètent que la solution dont ils disposaient déjà depuis deux ou trois ans. Ils affirment n'avoir ni les moyens, ni le temps, ni les personnels formés pour changer de solution. Cela constitue un vrai problème.

M. Philippe Latombe, rapporteur. Cela expliquerait en effet la volonté d'utiliser des systèmes préexistants intégrés. Avez-vous des remarques complémentaires à apporter sur tous les sujets que nous avons évoqués ?

Mme Pierrette Vidal. La souveraineté passe par deux axes : l'amélioration et l'accélération, certes, mais aussi l'indépendance. Il n'est pas normal que nous ne disposions pas de davantage de solutions françaises et européennes. Il faut construire ensemble cette indépendance. S'agissant des PC, nous ne pourrons pas rattraper notre retard : les équipements étrangers fonctionnent très bien et sont d'ailleurs validés par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). En revanche, de plus en plus de clients s'orientent vers des solutions françaises en matière de software. Cela fonctionne très bien. Je citerai les exemples d'Axway, de Tessi, de Doctolib. Il faut continuer à les promouvoir.

SCC est très vigilant à disposer de centres de service en France et à pouvoir contribuer à l'insertion sociale. Cela est d'ailleurs très demandé par le secteur public. Nous essayons de recruter un maximum en insertion sociale et nous ne sommes pas suffisamment aidés pour promouvoir ces emplois.

M. Michel Ferrand. Il me semble important de promouvoir les solutions françaises : Doctolib en est un exemple, mais il est important de promouvoir également d'autres entreprises, à ce stade moins développées et moins connues. Il faut continuer à les aider, et les aider encore davantage.

D'autre part, il faut s'assurer que les entreprises produisent en France. Des freins linguistiques comme des freins de compétences s'opposent parfois à l'installation des entreprises du secteur informatique en France. Je citerai l'exemple de Cap, qui est installée en Inde, certes pour des raisons de coût, mais aussi pour des raisons de compétences. Nous manquons de compétences en France. Il s'agit d'un choix de technologie, mais aussi du choix de nos ingénieurs de demain.

M. Edward Jossa. La souveraineté se conquiert encore plus qu'elle ne se défend, particulièrement dans le domaine informatique. Des interdépendances considérables existent entre le software, le hardware, le conseil et le logiciel. Cela nécessite une réflexion stratégique fine et poussée sur ces sujets. Il convient de promouvoir des solutions françaises ainsi que de promouvoir des solutions de protection de notre économie. Nous devons mobiliser pour cela tous les ressorts existants. Il faut soutenir les grandes entreprises françaises : vous avez cité Doctolib, Cap et Atos – il est vrai que ces entreprises ont en partie délocalisé leurs emplois, mais c'est aussi de cette manière qu'elles ont pu grossir et garantir leur croissance. Il est indispensable que nous disposions d'un certain nombre de grands champions français et européens et que nous soutenions leurs activités.

M. Philippe Latombe, rapporteur. Je vous remercie du temps que vous nous avez consacré et des éléments que vous avez bien voulu partager avec nous.

Audition de M. Nadi Bou Hanna, directeur interministériel du numérique, et de M. Michel Grévoul, directeur des achats de l'État *(21 janvier 2021)*

Présidence de M. Philippe Latombe, Rapporteur.

M. Philippe Latombe, rapporteur. Bonjour à tous. Notre mission d'information poursuit ses travaux avec l'audition de la direction des achats de l'État (DAE) et de la direction interministérielle du numérique (DINUM).

Notre objectif est d'échanger avec vous sur la façon dont la commande publique peut être mise au service de la transformation numérique de nos administrations et de la construction d'une souveraineté numérique nationale ou européenne.

Nous recevons ce matin M. Nadi Bou Hanna, directeur interministériel du numérique et M. Michel Grévoul, directeur des achats de l'État.

J'aimerais d'abord que vous nous fassiez part de ce que recouvre, selon vous, la notion de souveraineté numérique. Ce concept fait l'objet d'une attention croissante de la part des pouvoirs publics, notamment depuis la crise sanitaire. Nous avons, au cours de nos auditions, eu l'occasion de recueillir plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. Je suis intéressé par le regard que vous portez sur ce concept et la façon dont il peut, selon vous, se traduire concrètement au sein de l'action publique.

En second lieu, je souhaiterais échanger avec vous sur le contenu de la commande publique française et ses liens avec la promotion de notre souveraineté numérique. J'aimerais notamment savoir si l'État privilégie ou non, lorsque cela est possible, l'acquisition de matériels, de logiciels, de services numériques français ou européens. Je suis intéressé à connaître sur ce point votre analyse des forces et faiblesses de l'offre numérique française et européenne, et la façon de remédier à nos éventuelles carences.

Enfin, j'aimerais vous interroger sur la transformation numérique des acteurs publics, et plus particulièrement de l'État, puisque la DINUM et la DAE participent pleinement à ce processus d'ampleur. Je souhaiterais que vous nous présentiez la stratégie de l'État dans ce domaine, ainsi qu'un point d'étape sur la numérisation de nos administrations. Enfin, dans un contexte marqué par la recrudescence des cyberattaques en 2020, j'aimerais recueillir votre avis sur le niveau actuel de diffusion d'une culture de la cyberprotection au sein de la sphère publique.

Je vous cède maintenant la parole pour un propos liminaire d'environ dix minutes chacun, puis nous engagerons le dialogue sur la base des éléments que vous nous aurez apportés.

M. Nadi Bou Hanna, directeur interministériel du numérique. Je commencerai par vous présenter le système d'information et les actions numériques de l'État.

Le système d'information de l'État repose sur le principe de subsidiarité. Chaque ministre, appuyé par sa direction du numérique, en est responsable sur son périmètre. La direction interministérielle du numérique (DINUM), placée sous l'autorité de la ministre de la transformation et de la fonction publiques, Mme Amélie de Montchalin, assure la cohérence

d'ensemble, le portage stratégique en matière de numérique ainsi que l'animation de cette équipe. Nous jouons donc un rôle de capitaine d'équipe. Nous intervenons auprès du gouvernement pour le conseiller, pour assurer une coordination fonctionnelle des directions du numérique, pour partager les bonnes pratiques et pour contrôler l'exécution des grands projets informatiques. Ma direction intervient également en soutien à l'innovation, en appui et en animation des acteurs de la GovTech. Enfin, la politique de la donnée est un axe de force très important de notre activité, qui conditionne la maturation des politiques publiques ; la DINUM apporte un appui aux administrations sur la gestion de ce trésor.

La DINUM assure également un rôle de création et d'exploitation de solutions. La résilience de l'État dans le domaine du numérique est directement portée par ma direction, avec l'appui des autres directions du numérique. Cette résilience repose sur le réseau interministériel de l'État, mais aussi sur la mise à disposition de solutions numériques pour assurer la continuité du service public, même quand les agents travaillent à distance.

La DINUM a lancé en 2019 un programme d'accélération de la transformation numérique de l'État, nommé Tech.gouv. Ce programme vise à développer la simplification et l'inclusion numérique, l'attractivité de l'État (notamment comme employeur des profils du numérique), ainsi qu'à renforcer les alliances avec la société civile et les acteurs industriels. Ce programme a récemment donné lieu à la mise en place d'un sac à dos numérique pour les agents publics afin d'assurer la continuité d'exercice de leurs missions, ainsi qu'à la création d'un lab GovTech, prenant la forme d'un guichet d'échanges entre les acteurs français et européens et les porteurs de projets au sein de l'État. Nous avons également travaillé sur le développement de l'identité numérique, notamment au travers du dispositif France Connect, qui contribue à créer une réelle souveraineté de l'État en la matière. Nous avons enfin mis sur pied l'observatoire de la dématérialisation.

Pour conclure, ma direction est en charge de piloter une partie du plan de relance. Cette enveloppe de 500 millions d'euros doit servir à soutenir les projets de l'État en s'appuyant autant que possible sur l'écosystème numérique français et européen.

M. Michel Grévoul, directeur des achats de l'État. La direction des achats de l'État (DAE) définit la politique des achats de l'État, hors marchés de défense et de sécurité. S'agissant de la stratégie numérique, celle-ci est décidée par la DINUM ; la DAE met en œuvre et porte les marchés interministériels afférents au numérique. Néanmoins, de nombreux marchés demeurent traités en ministériel et n'ont pas recours aux marchés interministériels portés par la DAE.

La DAE poursuit cinq objectifs majeurs : tout d'abord, réaliser des économies d'achat et contribuer aux économies budgétaires liées aux achats de l'État ; faciliter l'accès des petites et moyennes entreprises (PME) aux marchés publics ; favoriser les achats d'innovation ; enfin, prévoir le recours aux dispositions sociales et environnementales dans les marchés publics.

À ce titre, la DAE est amenée à conclure des marchés interministériels. Pour cela, elle établit une programmation pluriannuelle des achats de l'État, disponible sur le site Internet de la DAE. Nous sommes le seul État européen à publier en ligne l'intégralité des projets d'achat des ministères à un horizon de quatre ans. Cette transparence constitue un moyen d'inciter les entreprises à s'inscrire sur notre plateforme dématérialisée des achats, nommée Place, sur laquelle sont publiées tous les marchés ministériels ainsi que les marchés interministériels portés par la DAE.

Je présenterai notre actualité en 2020 et 2021. La DAE a essentiellement été mobilisée pour répondre à la crise sanitaire, qui a eu des impacts numériques et généraux. La DAE a

porté des marchés pour les masques non sanitaires, c'est-à-dire les masques textiles lavables. Les achats sanitaires relèvent directement du ministère de la santé et de Santé publique France. L'achat de masques non sanitaires participe à renforcer les dimensions de l'État protecteur (pour venir en aide aux personnes précaires) et de l'État employeur (pour protéger ses agents).

La crise a causé des pénuries de matériel numérique. La fabrication de beaucoup de ces matériels ayant lieu en Asie, la fermeture d'usines a causé la rupture de plusieurs composants. Nous avons proposé à la DINUM de constituer un stock d'ordinateurs beaucoup plus important qu'à l'habitude, afin de limiter les risques de rupture d'approvisionnement du fait de la forte demande mondiale.

L'année 2021 marque le renouvellement d'un accord cadre interministériel sur les logiciels libres. Cela recouvre deux marchés interministériels : un marché de support et un marché d'expertise, qui seront lancés par la DAE.

Nous avons par ailleurs déjà lancé un marché de *cloud* cercle 3, comprenant les données non sensibles, en co-prescription avec la DINUM et l'UGAP. L'objectif est de faciliter la consommation de services de *cloud* public pour l'ensemble des acheteurs publics. Parmi les titulaires du marché, plusieurs sont français : OVH, Outscale, Orange business services.

Nous travaillons également, en partenariat avec la DINUM et l'Institut du numérique responsable, à la production d'un guide pratique pour un achat numérique responsable. Ce guide vise à la prise en compte des aspects environnementaux et sociaux dans l'achat de matériels et de services informatiques.

Nous mettons également en œuvre un accord-cadre interministériel d'assistance à maîtrise d'œuvre, qui vise à répondre aux besoins des bénéficiaires en matière de mise en œuvre des prestations intellectuelles informatiques. Cet accord-cadre a été conçu de manière à permettre à des PME de répondre aux marchés.

S'agissant de la souveraineté numérique, nous insérons des clauses strictes de conformité au règlement général sur la protection des données (RGPD) dans l'ensemble de nos marchés. Les acheteurs veillent donc à ce que les entreprises s'engagent à ce sujet.

Par ailleurs, tous les acheteurs respectent la politique de sécurité des systèmes d'information de l'État. Cela ouvre notamment la possibilité à certains marchés de bénéficier du label SecNumCloud.

Nous sommes enfin très attentifs aux clauses de réversibilité dans nos marchés interministériels, notamment quand celles-ci concernent les données.

M. Nadi Bou Hanna. Si vous me le permettez, M. le président, je complèterai mon propos par une définition de la souveraineté numérique. Il me semble que cette notion n'est pas définie dans les textes. Je m'appuie sur trois principes pour la définir.

Tout d'abord, le principe de liberté : il s'agit de la liberté de choisir ses fournisseurs, mais aussi de définir une stratégie puis d'en changer. D'une certaine manière, il s'agit de la liberté de choisir ses dépendances : de qui acceptons-nous de dépendre ?

Le second principe est celui de la maîtrise. Nous ne pouvons pas envisager de souveraineté numérique si l'État ne dispose pas des expertises qui permettent d'évaluer les

risques et les solutions ainsi que d'internaliser certaines fonctions. La souveraineté numérique n'est pas possible si une partie des fonctions les plus critiques ne sont pas internalisées.

Enfin, le principe de réversibilité : il s'agit de la possibilité de mettre fin à des projets, de changer de prestataire, sans se retrouver de fait pris dans une chaîne de dépendances sur laquelle nous n'avons plus de pouvoir.

Pour ma part, je n'aime pas recourir au concept de l'alignement des intérêts des parties prenantes. Cette notion est subjective et fluctuante dans le temps. L'on ne peut par conséquent pas baser une stratégie de souveraineté numérique sur un alignement ponctuel des intérêts.

Enfin, il me semble que la souveraineté numérique n'est pas un sujet de texte : ce sujet est avant tout présent dans les têtes. Certains porteurs de projets au sein de l'État font part d'une forme de fatalisme et de résignation. Ils tendent à considérer que le corpus de textes et de réglementations en vigueur – le code des marchés publics, notamment – se focalise uniquement sur la concurrence et briderait ainsi la prise en compte de tout autre enjeu, notamment économique ou d'influence. Je combats au quotidien cette posture. La souveraineté numérique suppose de responsabiliser collectivement les acteurs, afin de donner corps aux trois concepts de liberté, de maîtrise et de réversibilité qui sont au cœur de l'intérêt de l'État.

M. Philippe Latombe, rapporteur. Merci.

Nous avons précédemment auditionné l'UGAP et SCC. Ils constatent, au sein des administrations centrales et plus encore des collectivités locales, un manque de compétence et d'expertise qui rend possible l'adoption de solutions intégrées et globales, proposées par de grands acteurs.

Vous avez évoqué la réversibilité. Le Health Data Hub en est un bon exemple. Il a été demandé à l'UGAP de passer un marché avec Microsoft, sans effectuer de mise en concurrence. L'UGAP a exécuté l'ordre de commande reçu. Suite à la décision du Conseil d'État, la réversibilité a ensuite été annoncée à deux ans. Est-ce une vraie réversibilité quand elle intervient après deux ans ?

D'une façon plus générale, le code des marchés publics est perçu par l'essentiel des acteurs comme étant assez bridant. Quels sont les points qui, selon vous, pourraient faire évoluer l'acculturation des acteurs et des décideurs de la commande publique ? Quels sont les leviers à activer pour révéler les opportunités laissées ouvertes par le code de la commande publique pour favoriser d'autres types d'entreprises ?

M. Nadi Bou Hanna. Nous sommes obligés d'appliquer le principe de réalité et de composer avec les solutions présentes. De réels déséquilibres existent. Par exemple, deux systèmes d'exploitation (*OS*) dominent outrageusement le marché des *smartphones* – ils sont tous deux portés par des éditeurs américains. Le marché de la microinformatique et de la bureautique est également dominé à plus de 90% par un acteur, Microsoft. Le marché de la recherche sur Internet est dominé par un seul acteur, Google. Cela est la réalité.

Mon rôle au sein de l'État est de garantir que des solutions alternatives puissent émerger et se développer. Je prendrai l'exemple du moteur de recherches. Avec l'accord du gouvernement, j'ai mis en place une règle par défaut qui veut que l'ensemble des agents de l'État soient équipés, sur leur ordinateur et leur *smartphone* professionnels, d'un moteur de recherches alternatif, en l'occurrence Qwant, car celui-ci garantit mieux que les autres l'anonymat des recherches des agents publics et une certaine forme de neutralité du web.

Nous appliquons la même logique s'agissant des solutions de continuité de service. L'État a déployé, en partenariat avec une start-up franco-britannique, une solution de messagerie instantanée sécurisée, dont le code est ouvert, et nommée Tchap. Cette solution est utilisée par plus de 200 000 agents.

Nous poursuivons la même logique s'agissant des outils de visioconférence. Nous avons recours à des plateformes alternatives, soit commerciales, soit open-source, qui fonctionnent bien.

Nous travaillons également avec des PME françaises s'agissant des outils collaboratifs. Deux projets, Osmose et Resana, ont été lancés pendant la crise sanitaire et sont aujourd'hui utilisés au quotidien par plus de 100 000 agents publics. Le rôle de ma direction est de faire émerger des solutions et de les partager largement au sein des agents.

Cela n'est donc pas une fatalité – il n'existe pas uniquement les suites très intégrées, portées par de grands éditeurs américains, que vous mentionniez. L'usage de solutions alternatives nécessite certes davantage d'énergie, car il faut intégrer ensemble ces briques, mais il est possible. Et si cela est possible, nous le faisons.

M. Michel Grévoul. Depuis un an, l'urgence générée par la crise a constitué un formidable vecteur d'acceptation et d'accélération de l'usage de nouveaux outils de communication au sein de l'État. Les agents utilisent la messagerie sécurisée Tchap, ont recours à des solutions de visioconférence comme Jitsi ou à la solution interne Visiby ou Open Videopresence d'Orange.

S'agissant de la commande publique, nous souhaitons encourager les réponses des entreprises françaises et européennes à nos marchés. Nous avons ainsi largement insisté sur la possibilité ouverte aux entreprises de constituer des groupements pour y répondre. Nous constatons que des PME se regroupent, non seulement dans le secteur du numérique mais aussi des fournitures ou des travaux. Cette possibilité constitue donc un moyen pour des PME innovantes d'accéder à nos marchés.

Je répondrai à votre question portant sur le code de la commande publique et l'achat de prestations ou de matériels informatiques et numériques. L'État exploite pleinement les possibilités données par le code de la commande publique. Nous systématisons notamment le *sourcing*, qui consiste à opérer une veille sur les fournisseurs avant le lancement des marchés, maximisant ainsi les chances de recevoir un nombre important de réponses. Nous nous efforçons également de proposer des cahiers des charges les plus ouverts possibles, permettant à des variantes, différentes de notre offre de base, d'émerger. Nous espérons ainsi faciliter l'accès à nos marchés à des entreprises proposant des solutions disruptives et innovantes.

Nous avons par ailleurs mis en place un guichet unique des achats de l'État, accessible sur le site Internet de la DAE. Toute entreprise peut nous contacter *via* ce site. Nous identifions alors si les solutions proposées par cette entreprise sont innovantes ou standard, et nous l'orientons vers un acheteur spécialisé sur son segment de marché.

Vous nous avez interrogé sur l'opportunité de développer un droit de préférence pour les entreprises nationales du secteur du numérique. En l'état actuel du droit de la commande publique, qui se place en conformité avec les directives européennes, il n'est pas possible d'accorder une préférence à une entreprise sur la base de sa nationalité – excepté pour les marchés de défense et de sécurité. Un Small Business Act à la française n'est donc pas possible. Contrairement aux États-Unis, nous n'avons pas fait évoluer les règles de

l'Organisation mondiale du commerce (OMC) et nous ne pouvons pas réserver de marchés à des PME nationales.

M. Philippe Latombe, rapporteur. Cela fait effectivement partie des questions qui nous sont souvent adressées. L'article 2153-1 du code de la commande publique impose l'égalité de traitement entre les entreprises européennes et avec les entreprises liées par les accords extra-européens conclus dans le cadre de l'OMC. La Chine n'est pas partie à un tel accord au sein de l'OMC. En revanche, cela soulève la question du traitement des entreprises américaines. Certaines entreprises américaines créent des filiales dans des pays européens dans lesquels la pression fiscale est faible. Elles participent alors aux marchés publics européens, mais sans même contribuer à l'impôt au même titre que les autres. L'opinion publique et les entreprises sont de plus en plus sensibles à ces questions et l'idée d'un Small Business Act à l'européenne émerge.

L'UGAP a expliqué vouloir favoriser les PME, les startups et les très petites entreprises (TPE) françaises, mais vouloir également vérifier d'abord que celles-ci étaient suffisamment solides. Or, comment est-il possible de s'assurer que celles-ci sont suffisamment solides si elles ne peuvent pas bénéficier de la commande publique, qui leur permet de faire grossir leurs activités et d'atteindre une taille critique ? Pour l'acheteur, comment assurer la sécurité et la robustesse des solutions, et faire confiance à des TPE et PME à la structure financière parfois fragile ? Dans le même temps, les PME regrettent des délais longs de paiement de la commande publique, qui génèrent des problèmes de trésorerie. Existe-t-il des solutions pour concilier ces éléments ?

M. Michel Grévoul. Je répondrai à votre interrogation sur les délais de paiement. Je m'inscris totalement en faux contre les insinuations de retard de paiement de l'État. Le délai normal maximal de paiement est de 30 jours ; le délai moyen de paiement de l'État est inférieur à 20 jours. Je ne crois pas que la crainte d'un retard de paiement constitue aujourd'hui un frein pour les entreprises qui souhaitent répondre aux marchés publics.

M. Nadi Bou Hanna. Je m'inscris en faux contre le dogme selon lequel une entreprise doit être suffisamment solide pour accéder aux marchés publics. Cette approche est héritée des années 1990 et 2000, qui se caractérisaient par les grands projets, longs et onéreux. Les projets qui réussissent aujourd'hui, aussi bien au sein de l'État que des collectivités territoriales, sont des projets courts, qui mobilisent environ cinq personnes pour construire des solutions. Le succès des startups est significatif à ce sujet. Il faut d'abord commencer par prouver l'intérêt d'un produit avant d'atteindre une taille critique. Nous développons cette approche au sein du guichet GovTech et du programme Tech.gouv grâce à une mission nommée LABEL. Cette mission doit permettre d'identifier des solutions prometteuses, dont la plupart sont portées par des PME, et de déterminer si celles-ci sont capables de se conformer aux exigences de l'État. Il ne s'agit pas d'exigences de volumétrie ; mais bien de localisation d'hébergement ou d'interopérabilité des solutions.

Le code de la commande publique ouvre de nombreuses possibilités pour privilégier des solutions de cette nature. Un prescripteur peut, par exemple, choisir de monter un plateau de projet intégré, réunissant la maîtrise d'ouvrage, les développeurs, les designers de l'expérience utilisateur (UX). Cela constitue un choix stratégique visant à favoriser la réussite des projets. Mécaniquement, les acteurs de proximité seront privilégiés vis-à-vis des acteurs offshore. Si le prescripteur impose que le support d'une solution et la conduite du projet se déroulent en français, il oriente le positionnement des entreprises qui soumettront une offre. Lorsqu'un prescripteur impose une interopérabilité et une conformité à des référentiels mis en place en interministériel en France, il privilégie les acteurs qui ont fait l'effort de s'intéresser

aux marchés publics en France. Cela ne constitue donc pas la chasse gardée des grands groupes internationaux.

Nous constatons que beaucoup de PME saisissent l'opportunité de répondre aux marchés publics numériques portés par l'État en direct ou en regroupement. Ma direction a mis en place un marché transverse portant sur les besoins de coaching de l'ensemble des ministères sur les projets agiles. Nous avons fait le choix de privilégier les regroupements de PME et nous l'avons explicitement exprimé dans le cahier des charges. Il s'agit d'un choix stratégique du porteur de projet. Ces possibilités-là existent, mais il faut s'assurer qu'elles soient connues et utilisées.

De la même manière, l'achat innovant ouvre la possibilité aux porteurs de projet de retenir en direct une solution car ils sont intimement convaincus qu'elle est la meilleure solution pour répondre à un besoin innovant. Les possibilités existent, il faut simplement s'en saisir.

M. Philippe Latombe, rapporteur. Ma question porte sur le plan de transformation numérique de la commande publique, engagé pour la période 2017 – 2022. Pouvez-vous nous en présenter un point d'avancement ?

M. Michel Grévoul. Le plan de transformation numérique de la commande publique est porté spécifiquement par la direction des affaires juridiques (DAJ) de Bercy et par l'Agence pour l'informatique financière de l'État (AIFE). Ce plan vise à accroître l'efficacité de la commande publique par la dématérialisation et la numérisation. Les collectivités locales en font également partie ; la DAE y contribue mais elle n'est donc pas la seule associée.

Notre contribution porte essentiellement sur la programmation des achats et le *sourcing*. Nous mettons à disposition notre expérience en la matière, car l'État s'est doté d'un système d'information des achats complet. Il permet de suivre la commande publique d'un bout à l'autre de la chaîne : dès le *sourcing* en amont jusqu'à la passation des marchés puis au suivi de leur exécution. Le fait qu'un nombre croissant d'entités publiques se dote d'un système d'information des achats unifié permettra d'améliorer la qualité des achats.

S'agissant des outils numériques (postes de travail, ordinateurs, logiciels), la volonté de moderniser les outils et d'assurer leur résilience et leur sécurité s'est accélérée du fait de la crise. Nous sommes très sensibles à ces enjeux et nous avons travaillé avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) afin d'intégrer dans nos marchés des clauses concernant la cybersécurité.

Je reviendrai sur les marchés inférieurs à 100 000 euros pour lesquels il est prévu de pouvoir recourir à une solution innovante par une procédure de gré-à-gré et sans mise en concurrence. Cette latitude donnée aux acheteurs est très intéressante car elle leur permet de rapidement acheter un outil afin de procéder à une expérimentation. Mais l'acheteur doit être certain qu'il achète une vraie innovation. La DAE a ainsi créé un outil interne, diffusé au sein de l'État, l'Innov'score, qui permet grâce à un questionnaire à choix multiple de qualifier le degré d'innovation d'une solution. De la même manière, il est important que la hiérarchie reconnaisse un véritable droit à l'erreur à l'acheteur. Il est nécessaire que l'écosystème dans lequel il travaille accepte le risque de défaillance de fonctionnement ; car le risque fait partie intégrante de l'innovation. L'acceptation de la prise de risque inhérente à l'innovation ne relève pas d'une modification de texte ou de réglementation, mais d'un travail culturel. Les responsables de programme doivent reconnaître une prise de risque acceptable dans la mise en place d'une innovation.

Nous incitons les acheteurs qui doivent passer un marché, une fois le *sourcing* réalisé, à se poser la question suivante : plutôt que de lancer un marché avec des solutions standards, pourquoi ne pas réserver un lot de ce marché à une solution innovante ? Pour que cela soit possible, l'acheteur doit s'interroger sur son besoin bien en amont, c'est-à-dire six mois à un an avant le lancement du marché, de manière à disposer du temps nécessaire pour procéder à un test sur ces solutions. En ce sens, le décret du 24 décembre 2018 vise à faciliter, pour les marchés innovants inférieurs à 100 000 euros, un accès rapide à ces solutions.

Il existe également un autre outil très intéressant, utilisé par la DINUM aussi bien que par la DAE : il s'agit des appels à compétences, ou *request for information* (RFI). Ils permettent de conduire un *sourcing* de la manière la plus efficace possible. Pour cela, nous définissons un besoin et nous le portons à la connaissance de tous *via* nos outils d'information (Place ainsi que notre plateforme spécialisée sur les appels à compétences). L'écosystème s'agite alors pour satisfaire notre recherche. Cette procédure permet, avant de lancer un marché, de donner à voir les possibilités existantes, y compris les plus innovantes. Cela évite aux acheteurs de rédiger des cahiers des charges trop fermés.

M. Nadi Bou Hanna. Vous m'excuserez d'être un peu plus sévère que Michel Grévoul vis-à-vis du code des marchés publics. Ce dispositif repose sur un système de défiance. Au lieu de responsabiliser les porteurs de projets, il met en place un système de contrôle *a priori* plutôt que de transparence et de contrôle *a posteriori*. Cela était parfaitement justifié à l'époque où un certain nombre d'abus ont été détectés. Aujourd'hui, il construit une incitation au risque zéro. Michel Grévoul a très bien exprimé cette idée. L'État a consacré le droit à l'erreur pour les citoyens par la loi pour un État au service d'une société de confiance (ESSOC) ; il faut se permettre l'équivalent pour les porteurs de projets et les acheteurs. Il faut se permettre de prendre des risques en matière d'achats. Dans les années 1990, l'on disait qu'un bon directeur des systèmes d'information ne faisait jamais d'erreur quand il choisissait IBM pour ses grands projets. Un credo similaire existe encore aujourd'hui.

La politique du risque zéro nous conduit à des situations incompréhensibles. Vous évoquiez tout à l'heure l'expertise mobilisable des collectivités territoriales en matière informatique. Ma direction anime un dispositif de coopération avec les collectivités territoriales. Nous aimerions, autant que possible, partager avec elles des solutions développées ou achetées par l'État. Les juristes spécialisés au sein de l'État nous expliquent que cela pourrait être contraire au droit de la concurrence et pourrait mettre l'État en grave difficulté. Il faut absolument résoudre ces situations pour que l'intelligence des achats et l'intelligence des porteurs de projets priment au-delà du strict respect du droit et de l'interprétation du niveau de risque qui en découle.

Je souhaite aborder un autre point qui me paraît constituer un levier important pour développer les coopérations et la souveraineté numériques : il s'agit du logiciel libre.

M. Philippe Latombe, rapporteur. Je voulais effectivement vous interroger à ce sujet. Dans son rapport, Éric Bothorel avait justement proposé la création d'une mission sur le logiciel libre au sein de la DINUM.

Je souhaite également revenir sur les données. Vous avez évoqué ce « trésor » que représentent les données au sein de l'administration. Comment envisagez-vous leur stockage, leur valorisation et leur utilisation dans les conditions les plus respectueuses possibles de la souveraineté ?

M. Nadi Bou Hanna. Depuis le 23 décembre 2020 et la remise du rapport d'Éric Bothorel, je passe une partie importante de mes journées à construire la mise en œuvre de ses

recommandations, qui me paraissent essentielles pour l'État. Une grande partie d'entre elles, d'ailleurs, dépasse le strict champ de la donnée ou des codes sources. C'est le cas des compétences de l'État en matière de numérique : cette question entre en résonance directe avec le programme Tech.gouv et constitue un coup de projecteur important sur nos actions.

Je reviendrai aux données et aux codes sources. Ces deux notions cousines se traitent de manière différente.

Il est évident que le partage de la donnée entre les administrations contribuerait directement à la simplification des démarches pour les citoyens. Il s'agit du principe du « dites-le nous une fois » : si la donnée existe dans la sphère fiscale, il est absurde que l'État la demande à nouveau dans la sphère sociale, alors que la donnée est facilement partageable. Le premier champ essentiel concerne donc la circulation de la donnée au sein de l'État. En plus de simplifier la vie des Français, cette circulation permettrait de construire des politiques publiques proactives. Pourquoi demander à un citoyen de conduire une démarche, alors que l'État sait, par exemple, qu'il est bénéficiaire par défaut d'une prestation sociale ? Une nouvelle politique publique plus motrice pourrait donc se construire en partageant mieux la donnée au sein de l'État.

La donnée prend également beaucoup de valeur quand elle est partagée avec l'écosystème qui gravite autour de l'État : la société civile, les entreprises du numérique ou les individus. Pendant la crise sanitaire, on a constaté que la transparence des données en matière de contamination était essentielle. L'État publie les données de contaminations et les rend largement partageables afin que de nouveaux services puissent éventuellement se développer à l'initiative de la société civile. La mise à disposition des données permet ainsi leur valorisation.

L'approche du logiciel libre se développe depuis plusieurs décennies déjà. Dans certains champs, il est devenu la référence : c'est le cas des OS des infrastructures ou de l'hébergement du web. Ce levier favorise le partage. J'expliquais tout à l'heure qu'il était extrêmement compliqué, du point de vue du droit, de partager des solutions entre l'État et les collectivités territoriales. En revanche, il est très simple de le faire avec des logiciels libres. Si l'État produit un logiciel libre et qu'il choisit de reverser le code qui a été élaboré par ses services en open source pour que d'autres puissent s'en servir à nouveau (des collectivités territoriales ou bien des entreprises) et qu'ils enrichissent ce socle, alors tout le monde est gagnant. Le logiciel libre revêt donc un potentiel important. Il ne faut pas pour autant être naïf : des enjeux économiques majeurs existent en la matière. Des sociétés ont fondé leur modèle économique sur les services existants autour du logiciel libre. Au début des années 2000, certains pouvaient encore avoir l'illusion que le logiciel libre était gratuit. Ce n'est pas le cas. En revanche, il permet potentiellement de partager. Et ce partage a beaucoup de valeur.

Si le logiciel libre permet de partager, des solutions propriétaires le peuvent également, à la condition qu'elles se conforment aux bonnes pratiques édictées par l'État. Il s'agit en particulier de la mise à disposition d'interfaces de programmation d'application (API), qui permettent de consommer directement les données dans les logiciels ou de déclencher des transactions et offrent l'interopérabilité des solutions. Plusieurs leviers rendent donc possible la transformation numérique : ces leviers s'appuient aussi bien sur l'écosystème du logiciel libre, que l'État a tout intérêt à soutenir, que sur l'écosystème des éditeurs privés, qui ont adopté un autre modèle économique mais qui sont également en mesure de proposer des solutions extrêmement attractives et très ouvertes.

M. Philippe Latombe, rapporteur. Vous avez tous les deux fait part de la nécessité, pour les acheteurs, de prendre des risques. À cet égard, comment percevez-vous l'émergence

de nouveaux outils numériques, comme la *blockchain*, et leur utilisation ? Faut-il que ces outils connaissent un temps d'acculturation long dans les sphères privées avant que le public ne s'en saisisse ? La sphère publique peut-elle au contraire s'en emparer dans leur phase émergente et en expérimenter les usages ? Comment l'État gère-t-il l'expérimentation et quel est le niveau de prise de risque acceptable selon vous ?

M. Nadi Bou Hanna. S'agissant des technologies non matures, l'État a intérêt à tester des cas d'usage le plus tôt possible plutôt que de laisser le marché se structurer, ce qui se fait souvent au détriment des écosystèmes français. Mais cela ne concerne pas seulement le soutien aux filières. Cela recouvre un enjeu de maturation des pratiques au sein de l'État au bon moment. Nous ne pouvons pas perpétuer un modèle dans lequel l'État s'approprie, avec cinq ou dix ans de retard, des technologies que des entreprises privées ou d'autres États ont testées.

Je ne vous donnerai malheureusement pas beaucoup d'éléments positifs au sujet de la *blockchain*. L'État se situe sur un tiers de confiance par défaut et l'émergence de tiers de confiance externes ne s'est pas avéré judicieux jusqu'à présent. Nous n'avons pas développé beaucoup de cas d'usage intéressants sur la *blockchain*, et elle n'est par conséquent pas la technologie la plus portée.

En revanche, ma direction a fortement soutenu le développement de l'intelligence artificielle. Nous avons monté, notamment avec le soutien du Programme d'investissements d'avenir (PIA), un dispositif de financement des projets conduits par les ministères en la matière. Il s'agit souvent de projets exploratoires, conduits en liaison directe avec quelques entreprises expertes en la matière. Un certain nombre de ces expérimentations ont montré l'intérêt de les faire passer à l'échelle. Le sujet de la *data science* entre en résonance directe avec le sujet de la donnée – il en est une composante essentielle. L'intelligence artificielle se développe véritablement aujourd'hui au sein de l'État. La direction générale des Finances publiques (DGFiP), les douanes, Pôle Emploi, les acteurs de la sphère sociale sont, par exemple, en train de constituer des lacs de données (*data lakes*), c'est-à-dire des entrepôts de données, et d'y embarquer des solutions qui leur permettront d'exploiter ces données afin de prendre de meilleures décisions. Fondamentalement, l'État poursuit une politique d'innovation car celle-ci permet d'améliorer son fonctionnement et d'éclairer la prise de décision publique. Ma direction est évidemment motrice en la matière.

La composante « transformation numérique de l'État » du plan de relance prévoit d'ailleurs une enveloppe dédiée aux technologies non matures. Celle-ci permet un soutien direct et une prise en charge à 100%, dans une enveloppe limitée, des projets et des prototypes qui s'appuieraient sur des technologies non matures.

M. Philippe Latombe, rapporteur. Je vous interroge à ce sujet car le recours à Palantir pour aider l'État dans une partie très régalienne de ses missions a déclenché une grande polémique. Le fait que Palantir s'intègre maintenant dans GAIA-X alimente également un débat d'actualité très fort. Par ma question sur les besoins de l'État en technologies non matures, je cherchais à savoir dans quelle mesure des joueurs français ou européens auraient pu se substituer à ces sociétés étrangères.

M. Nadi Bou Hanna. À ma connaissance, Palantir n'est pas utilisé par l'État. Je n'ai évidemment pas visibilité sur l'ensemble des projets, mais s'il l'est, cela est à titre marginal. L'État a bien veillé à se doter de capacités en propre ou en appui d'entreprises européennes pour maîtriser sa donnée et essayer d'en définir les trajectoires. Je ne suis pas pleinement compétent en la matière et le mieux, à ce sujet, serait d'interroger les ministères sociaux ainsi que le ministère de l'intérieur.

M. Philippe Latombe, rapporteur. Nous ne manquerons pas de le faire. À ce stade, souhaitez-vous aborder des points nouveaux ou approfondir certains éléments évoqués précédemment ?

M. Michel Grévoul. Il est nécessaire d'encourager les acheteurs à adopter des comportements innovants. Pour cela, ils doivent être sécurisés dans leur position. Ils doivent donc pouvoir prendre des risques sans en être inquiétés par leur hiérarchie. Je rejoins les propos tenus par M. Nadi Bou Hanna : l'objectif de l'État est d'acheter des choses utiles pour l'État et pour les utilisateurs, que ceux-ci soient l'ensemble de la population, une population ciblée ou les agents. Parfois, il est nécessaire de tester une innovation pour savoir si elle est vraiment utile. Si la hiérarchie n'autorise pas cette prise de risque, de nombreux acheteurs craindront d'expérimenter la nouveauté et n'achèteront pas de produits innovants. Ce problème ne se réglera pas par l'évolution des lois ou des textes, mais par un travail quotidien au sein des directions des achats et de la DINUM, autorité prescriptrice. Ce travail doit porter sur l'évolution des pratiques des donneurs d'ordre, compétents en matière d'achats de services et de fournitures informatiques et numériques pour l'État.

M. Philippe Latombe, rapporteur. Je poserai une dernière question d'ordre juridique. Quelle vision portez-vous sur l'arrêt Schrems II de la Cour de Justice de l'Union Européenne (CJUE) et sur la décision du Conseil d'État concernant le Health Data Hub ? Cette décision demande la réversibilité et requiert un fournisseur européen à horizon de deux ans. En vérité, le Conseil d'État n'avait pas prévu ce délai de deux ans, c'est le ministère de la santé qui l'a demandé. Quelle vision avez-vous de ces deux décisions de justice et quelles conséquences en tirez-vous ?

M. Nadi Bou Hanna. Permettez-moi, avant de répondre à cette question, de revenir sur votre précédente demande.

Nous ne pouvons pas envisager de souveraineté numérique si nous ne sommes pas en mesure d'internaliser des compétences stratégiques au sein de l'État. Nous avons peu évoqué cet enjeu jusqu'à présent. La souveraineté repose sur la maîtrise et la compréhension des enjeux, des architectures, des grands projets. La Cour des comptes s'en est émue dans un rapport extrêmement bien documenté et retraçant les trajectoires de ces dernières années. Je constate que 90% à 95% de la maîtrise des grands projets ou des technologies est aujourd'hui externalisée. Les couches d'externalisation s'empilent : elles impliquent des grands cabinets de conseil, l'assistance à maîtrise d'ouvrage, l'entreprise de maîtrise d'œuvre, l'opérateur externe… Au final, l'ordonnateur ne dispose pas d'une vue d'ensemble et ne maîtrise pas le dispositif. Il perd la main. Aucune forme de souveraineté numérique ne peut alors se développer.

Évidemment, je ne défends pas l'idée qu'il faudrait absolument tout internaliser au sein de l'État. Cela serait absurde et non réaliste. Mais cela rejoint les enjeux actuels de la transformation de l'informatique. Les systèmes d'information, dans les années 1980 et 1990, étaient perçus comme des centres de coûts : ils étaient une commodité. Aujourd'hui, ils sont plutôt des leviers de transformation. Si aucun investissement n'est opéré dans ces leviers de transformation, ils resteront lettre morte.

J'en reviens à votre question d'ordre juridique. L'arrêt Schrems II est un arrêt stratégique, et il rejoint directement les réflexions conduites au sein de l'État. Nous sommes en train, depuis plusieurs mois déjà, de définir une nouvelle doctrine du *cloud* au sein de l'État. Ces travaux devraient aboutir dans les prochaines semaines. Cette doctrine du *cloud* vise à définir les règles du jeu pour l'État. Le cadre européen définit un cadre auquel l'on ne peut pas déroger. Pour autant, chacun des porteurs de projets et des États membres peut définir sa

doctrine, c'est-à-dire la manière dont il s'approprie ce cadre réglementaire et dont il l'incarne dans une stratégie. Cette doctrine du *cloud* aura justement vocation à garantir que l'hébergement des données – qu'il s'agisse des données des citoyens ou des données liées à l'activité essentielle des agents publics – ne pourra pas être localisé sur des plateformes faibles d'un point de vue de la sécurité, non conformes au RGPD ou qui ne garantissent pas leur étanchéité aux réglementations extra-européennes. Nous sommes donc en train d'inaugurer une nouvelle ère au sein du *cloud* de l'État. Celle-ci ne consiste pas simplement à nous assurer que des offres émergent, mais plutôt à nous assurer que les administrations s'en saisissent, qu'elles l'utilisent à bon escient, et que cela change la manière de concevoir et de produire des applications.

Vous avez évoqué le Health Data Hub. Comme je l'ai expliqué tout à l'heure, nous sommes confrontés à la réalité du marché. Le projet du Health Data Hub revêt un enjeu politique majeur et affichait un échéancier non négociable. Lorsque ce projet a été lancé, la seule plateforme qui était techniquement compatible avec l'ambition du projet, tel que cela a été analysé par le ministère de la santé, était celle de Microsoft. Depuis, des travaux ont été conduits. Nous avons notamment vu des hébergeurs agréés SecNumCloud mettre à niveau leurs plateformes. Nous assistons donc à un travail de mise à niveau des plateformes pour se conformer au besoin du client. Sur un projet de cette nature, nous n'allons pas dégrader ni le besoin client, ni la promesse politique. Les équipes techniques sont bien obligées de trouver les solutions techniques adéquates pour donner corps à cette promesse. Nous voulons envoyer au marché, et notamment aux hébergeurs européens, le signal suivant : à partir du moment où les règles du jeu seront bien déterminées, et que le marché sera réellement ouvert, les hébergeurs devront probablement travailler pour monter à niveau sur quelques fonctions, et alors être capables d'être compétitifs vis-à-vis des plateformes pour répondre à un projet d'envergure comme celui du Health Data Hub. Il n'y a pas de dogme s'agissant du Health Data Hub – il y a simplement un constat de réalité. Le souhait de l'ensemble des parties est que de nouvelles offres d'hébergement puissent émerger, qui remontent les couches, c'est-à-dire qui ne se contentent pas du niveau le plus bas (l'infrastructure) mais qui soient capables de remonter au niveau de la plateforme et des services à valeur ajoutée. Du côté du Health Data Hub, des ajustements doivent également être faits pour ouvrir davantage le champ de la concurrence. Nous y travaillons actuellement. Ma direction intervient en soutien du ministère de la santé pour définir une trajectoire de réelle mise en concurrence de la plateforme. Je ne peux pour l'instant pas vous dire si cela pourra se faire à un horizon de 18 mois, de 24 mois, ou plus. La réalité technique et la maturité des offres montreront, *in fine*, si ce plan de migration était réaliste.

M. Philippe Latombe, rapporteur. Merci du temps que vous nous avez consacré et des propos très éclairants que vous avez partagés avec nous. Nous sommes très impatients de prendre connaissance de la doctrine du *cloud* de l'État dès qu'elle sera achevée, car cela concerne directement les enjeux de notre mission d'information. Nous aurons peut-être alors l'occasion de vous auditionner à nouveau à ce sujet.

Audition commune de M. Stéphane de la Rosa, professeur de droit public à l'Université Paris-Est Créteil, de Me Thierry Dal Farra, avocat associé du cabinet UGGC Avocats, et de M. François Benchendikh, maître de conférence en droit public à Sciences Po Lille
(28 janvier 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Notre mission d'information achève aujourd'hui son cycle d'auditions consacrées à la commande publique par une table ronde rassemblant plusieurs juristes. Nous avons entendu ces dernières semaines des acteurs privés et publics. Il nous semble aujourd'hui important de parcourir le champ des possibles, l'objectif étant de mieux protéger et promouvoir la souveraineté numérique aux niveaux national et européen.

M. Philippe Latombe, rapporteur. J'évoquerai en introduction trois sujets. Premièrement, je souhaiterais que vous présentiez brièvement le droit de la commande publique et ses principales évolutions ces dernières années. Un certain nombre d'initiatives ont été prises pour moderniser la commande publique. Je pense, à la fois, au plan de transformation numérique engagé pour la période 2017-2022, à la loi d'accélération et de simplification de l'action publique du 7 décembre 2020 (loi ASAP), et aux mesures prises pour encourager le recours à davantage de solutions innovantes. Quel regard portez-vous sur ces éléments ? En second lieu, quelles sont, selon vous, les évolutions envisageables ou souhaitables du droit de la commande publique, afin de promouvoir, par son truchement, notre souveraineté numérique ? J'aimerais en particulier savoir s'il existe déjà des outils permettant de favoriser l'achat par des acteurs publics de matériels et de logiciels souverains. Si tel n'est pas le cas, quelles devraient être les caractéristiques d'un nouveau régime juridique allant dans ce sens, en conformité avec le droit européen ? Nous sommes ouverts à toutes vos propositions à cet égard. Enfin, j'aimerais que vous vous exprimiez plus globalement quant à l'influence des règles actuelles de la commande publique sur la capacité des acheteurs publics à prendre des risques dans leurs pratiques d'achats. La semaine dernière, si le directeur interministériel du numérique, M. Nadi Bou Hanna, nous a indiqué que le code de la commande publique pouvait être « désincitatif », la direction des achats de l'État ne semblait pas tout à fait en accord. Partagez-vous ce constat ? Des modifications sont-elles envisageables pour lever les obstacles qui semblent exister sur ce sujet ?

Pr Stéphane de La Rosa, professeur de droit public à l'Université Paris-Est Créteil. Les enjeux de souveraineté numérique nous obligent à réfléchir à l'adéquation des outils actuels de commande publique au besoin d'autonomie stratégique en matière de commande publique et de souveraineté. Ces enjeux croisent bien entendu l'évolution du droit de la commande publique, dans une perspective à la fois nationale et européenne.

L'articulation entre le droit de la commande publique et les activités numériques est essentielle. Le numérique est omniprésent dans de nombreux marchés publics de fourniture de matériels informatiques, de logiciels et de systèmes d'information. Nous saisissons également le numérique comme lot ou comme composante de marchés globaux. Nous le trouvons enfin dans nos contrats de concessions pour les transports ou la mobilité. L'omniprésence du numérique permet de prendre conscience de notre situation de forte dépendance vis-à-vis des géants du numérique ou d'États tiers. Cette dépendance s'illustre dans la rédaction de certains avis de marché. Par exemple, nous observons sur la base en ligne des avis de marché européens que des acheteurs demandent des solutions uniquement Microsoft ou bien des logiciels précis.

La rédaction d'avis de marché peut poser des problèmes de spécifications techniques ou même de rupture d'égalité.

Nous avons également pu observer cette dépendance dans le Health Data Hub, le grand contrat par lequel le ministère de la Santé a confié à Microsoft, sans véritable appel d'offres, le soin de stocker des données de santé, le risque étant que ces données soient transférées aux États-Unis. Cela s'est fait en méconnaissance de la jurisprudence *Schrems* de la Cour de justice, qui a indiqué qu'il n'existait pas de sécurité totale des données pour les usagers européens, si celles-ci sont transférées aux États-Unis.

Afin de limiter la situation de dépendance, réelle, vis-à-vis des grands acteurs du numérique, il existe déjà un certain nombre d'outils, mais ils sont sans doute mal ou insuffisamment exploités. Premièrement, les acheteurs publics pourraient être accompagnés dans la rédaction des clauses d'appel d'offres et des spécifications techniques. Ce travail devrait être mené pour tous les marchés numériques ou informatiques. Il serait également souhaitable d'affiner la rédaction des conditions d'exécution du marché. Par exemple, aux termes de l'article L. 2112-4 du code de la commande publique, l'acheteur peut exiger une localisation de tout ou partie du marché sur le territoire des États de l'Union européenne, afin de prendre en compte, notamment la sécurité des informations ou des approvisionnements. Ces outils sont peut-être mal connus, mais ils existent et peuvent guider une approche plus fine des acheteurs publics en matière de souveraineté numérique. Il existe également des outils de droit permettant de défendre une préférence communautaire pour certains achats. Ils se limitent aux secteurs en réseaux, c'est-à-dire les marchés d'infrastructures dans les domaines de l'eau, de l'énergie et des transports. Les marchés sont conclus par des entités adjudicatrices. Il est possible, sur le fondement du droit européen, de faire valoir un droit de préférence pour les offres européennes en excluant des offres qui ne seraient pas composées à plus de 50 % de produits ou de services européens. Ce système est intéressant, mais il ne peut être mis en œuvre que si le soumissionnaire, issu d'un État tiers, n'est pas partie à l'accord sur les marchés publics de l'OMC ou n'est pas partie à un accord bilatéral qu'aurait conclu l'Union européenne et qui donnerait un droit similaire d'accès préférentiel au marché.

Si ces outils existent, force est de reconnaître qu'ils demeurent assez limités. Cela incite les législateurs nationaux, dont la France, à s'engager dans l'élaboration de solutions strictement nationales, afin de privilégier les opérateurs internes du numérique. Tel est le cas de la loi ASAP du 7 décembre 2020 qui prévoit un mécanisme de relèvement des seuils à 100 000 euros jusqu'en 2022, ainsi que des dispenses de publicité et de mise en concurrence. Justifiées par un motif d'intérêt général, ces dispositions permettent d'attribuer directement le marché et de favoriser ainsi certains opérateurs. Ces mesures sont intéressantes, car elles sont rapidement applicables par les acheteurs. Suivant ce dispositif, il est possible de privilégier un opérateur européen du numérique. Néanmoins, je ne suis pas tout à fait certain qu'il soit conforme au droit européen de la commande publique. L'interprétation que la Cour de justice fait du principe de transparence implique des mesures de publicité et de mise en concurrence pour des marchés qui présentent un intérêt transfrontalier certain. Par exemple, s'agissant d'un marché de 100 000 euros localisé à Lille ou à Strasbourg, je ne sais pas si ce dispositif passerait avec succès le filtre de la jurisprudence européenne. Cela montre qu'on se situe à la limite de ce qu'on peut faire par rapport au droit européen avec des réponses qui seraient strictement nationales en la matière.

À partir de ces observations, il est nécessaire de mieux penser à l'échelle européenne un système de priorité en faveur d'opérateurs européens dans les marchés publics, en particulier dans le numérique. Comment et par quelles voies ? Tout d'abord, il convient d'engager une réflexion sur les conséquences de l'appartenance à l'accord sur les marchés

publics (AMP) conclu dans le cadre de l'OMC. Je rappelle que les règles de calcul des seuils sont issues de l'AMP, qui est révisé tous les deux ans par référence à la valeur des droits de tirage spéciaux. Ces variations de seuils sont ensuite reprises par la Commission, puis reprises par les États membres pour le calcul de leurs seuils de passation. Il s'agit donc bien d'un instrument qui nous lie quant à ces questions de seuils. Il nous lie également concernant la clause d'exigence de la nation la plus favorisée, qui suppose, en application de l'accord, que nous donnions la même préférence aux opérateurs français, européens ou tiers, dès lors qu'on a conclu l'AMP ou un accord bilatéral reprenant des stipulations identiques. Engager une réflexion sur l'AMP me semble d'autant plus nécessaire que l'administration Biden vient de réactiver le *Buy American Act* qui prévoit un système de préférence aux entreprises américaines sous les seuils issus de l'AMP. Il permet également un achat préférentiel de biens à plus de 50 % d'origine américaine. Le *Buy American Act* pourrait également se déployer sous les seuils formalisés issus de l'AMP. Dans sa présentation du décret présidentiel diffusée sur le site de la Maison-Blanche depuis le 25 janvier, la nouvelle administration américaine indique clairement qu'elle souhaite réengager une négociation relative à l'AMP sur la question de la préférence interne. Ce champ doit donc être investi par le législateur français et par les institutions européennes.

La deuxième voie concerne l'extension du régime de préférence des produits à plus de 50 % d'origine européenne, que j'ai présenté dans mon rapport. Pourquoi ne pas étendre ce dispositif à l'ensemble des marchés publics au lieu de le limiter aux secteurs en réseaux ? Cette voie ne pourra être suivie qu'en concordance avec une révision de l'AMP.

En troisième lieu, la Commission a conçu des systèmes de réciprocité par rapport aux États tiers. Une proposition a été émise en 2012, une deuxième en 2016. Un livre blanc est paru sur les distorsions de concurrence étrangère. Aucun texte précis ne détermine aujourd'hui si nous pourrions fermer nos marchés en cas de concurrence déloyale d'États tiers. Ce thème pourrait être approfondi.

En ce qui concerne les marchés innovants, le système de 2018 pourrait être une bonne solution, mais les acheteurs ne se le sont pas pleinement approprié, certains craignant la requalification des marchés innovants en marchés classiques de la commande publique, avec le risque de contentieux que cela entraînerait. En tout cas, une réflexion devra être menée sur l'usage de ce dispositif avec le partenariat d'innovation issu des directives et qui peut également permettre des marchés innovants. Le dispositif pourrait éviter un effet de dispersion.

M. François Benchendikh, maître de conférences en droit public à Sciences Po Lille. La situation venant d'être décrite à l'échelle européenne, je porterai mon analyse au niveau national. Le droit de la commande publique se trouve formalisé dans un code établi en avril 2019, qui soulève certaines questions concernant les outils informatiques. Le droit de la commande publique a été longtemps instable. Plusieurs codes se sont succédé, en 2001, en 2004, puis en 2006, ce qui illustre le caractère difficile à appréhender de ce droit. Lorsque nous discutons avec des chefs d'entreprise, certains disent même qu'ils ne souhaitent plus répondre à un appel d'offres, car le coût de compréhension de la matière juridique, le temps que cela représente, rapportés à la faible chance d'obtenir l'offre, peuvent s'avérer dissuasifs. Il est important de garder à l'esprit que ce droit est susceptible d'évoluer souvent.

La seconde caractéristique de ce droit est d'être paradoxal. D'un côté, il énonce des principes fondamentaux rappelés à la fois par la jurisprudence de la Cour de justice, par le Conseil d'État et par le Conseil constitutionnel. Ce sont notamment les principes d'efficacité de la commande publique, de la protection et de la bonne utilisation de la donnée publique. Les notions de transparence et d'égalité de traitement sont également défendues. De l'autre,

le droit de la commande publique énonce des éléments d'une grande précision concernant les délais ou les seuils qu'il est indispensable de connaître, lorsqu'on répond à un appel d'offres. L'écart des grands principes aux détails concrets requiert une attention particulière.

Un premier élément essentiel est l'information des agents publics et des entreprises innovantes. Leurs capacités à concevoir et à structurer un cahier des charges, à rédiger des clauses, à déposer une offre en relation avec l'objectif du marché, sont déterminantes. Lorsqu'une commune de 5 000 habitants cherche à se doter d'un outil informatique innovant, la difficulté est de trouver des agents publics capables de formaliser l'offre. L'accompagnement des maîtres d'ouvrage publics est donc une caractéristique importante. Les observatoires régionaux de la commande publique sont des structures intéressantes. Ils peuvent à la fois accompagner les collectivités et faire office de cellules de réflexion. Les chambres des métiers et les chambres de commerce et d'industrie peuvent également mener des travaux sur le sujet. L'enjeu est la capacité à intervenir au sein du territoire.

Le deuxième élément important est la capacité des services de l'État. Depuis quelques années, ils sont structurés en de nouvelles directions, telles que la direction interministérielle du numérique (DINUM). L'État est détenteur d'une expertise poussée qui doit être sollicitée vis-à-vis des marchés publics.

En troisième lieu, il convient de détailler la relation entre la souveraineté numérique et la notion d'économie circulaire. Il est très important de pouvoir innover sur les territoires à ce niveau. Par exemple, l'hôpital de Metz conduit une réflexion sur la chaleur numérique. On peut également s'intéresser au recyclage des appareils électroniques. La capacité à localiser des entreprises innovantes sur le territoire national me semble déterminante.

Les différents plans de l'État, tels que le plan quantique annoncé par le chef de l'État ou le plan France très haut débit, offrent la possibilité d'obtenir des budgets significatifs pour avancer sur ces questions. Enfin, les centres de données *(data centers)* publics, qui permettent de localiser une information numérique sur le territoire national ou européen, sont un moyen pour les entreprises françaises ou européennes d'obtenir des marchés. Pour des raisons de sécurité publique, la maîtrise du stockage par les services de l'État, les universités et les établissements publics hospitaliers, est fondamentale. Il est important de pouvoir exiger que les données demeurent sur le territoire national ou européen.

Enfin, le *Buy European Act* est un enjeu crucial qui doit être appréhendé avec l'AMP au sein de l'OMC. L'alternative est soit de fermer quelques portes aux entreprises américaines et chinoises, soit de se montrer plus diplomate et d'inviter les États tiers à accueillir favorablement les outils numériques européens et nationaux.

Me Thierry Dal Farra, avocat associé du cabinet UGGC Avocats. Je souscris pleinement à l'analyse juridique et aux préconisations qui viennent d'être formulées. J'exposerai pour ma part le point de vue du praticien. J'ai accompagné des maîtres d'ouvrage informatique importants, notamment le projet Chorus, le projet d'opérateur national de paye, l'informatisation de l'AP-HP et les systèmes d'information clinique. J'accompagne aujourd'hui l'agence du numérique en santé. Mon point de vue est plutôt celui des grands maîtres d'ouvrage informatiques.

L'objectif de souveraineté numérique soulève deux grandes questions. La première, d'ordre économique, consiste à se demander comment l'achat public peut contribuer à l'émergence d'une offre économique orientée vers l'autosuffisance et qui permette aux acheteurs publics, lorsqu'ils lancent de grands projets informatiques, d'accéder à une offre française ou européenne crédible face à celle des grands opérateurs ou éditeurs américains.

L'achat public peut aider à atteindre l'objectif économique d'autosuffisance, mais de manière assez limitée, car comme l'a rappelé le Pr Stéphane de La Rosa, les politiques de préférence nationale se heurteront au droit européen et pourront difficilement faire obstacle au choix de l'offre économiquement la plus avantageuse. Un acheteur public souhaite d'abord acquérir le meilleur système. L'acheteur public fait une politique de la demande. Or, aucune politique de la demande ne peut remplacer une politique de l'offre. En économie, c'est plutôt l'offre qui crée la demande. L'acheteur public émettra bien entendu des besoins, mais il ne peut pas les formuler trop à l'avance à l'égard de certains opérateurs, car cela constituerait une sorte de favoritisme par détention d'informations privilégiées. Il s'agit d'une politique de demande émise 52 jours avant le dépôt des offres.

Dans l'affaire Chorus, l'État a voulu acquérir un logiciel qui traduisait la LOLF (loi organique relative aux lois de finances) pour la gestion des fonds publics. Le ministère des Finances voulait absolument un marché à l'éditeur, et pas un marché où il y ait des prestations d'intégration qui rendraient le dispositif difficilement maintenable. Par conséquent, nous nous sommes demandé comment faire pour contacter les grands éditeurs afin de les inviter à réfléchir aux besoins. J'ai eu l'idée de faire publier sur le site internet du ministère une espèce de politique d'orientation précisant nos besoins et notre volonté d'obtenir un marché à l'éditeur. Il s'agissait bien entendu d'une information un peu privilégiée sur les intentions d'achat. Les modalités de publicité se sont avérées quelque peu empiriques. Une nouvelle fois, c'est une politique de la demande, ce n'est pas une politique de l'offre. Il n'y a pas de politique de la demande qui puisse suppléer une politique de l'offre.

L'autre objectif de la souveraineté numérique est plus juridique. Il s'agit d'une approche complémentaire qui consiste à contribuer à l'indépendance, à la sécurité des traitements, à la protection des données et des intérêts essentiels de l'État et des Français. Or, sur ce point, les leviers ne se situent pas au stade de la passation, mais au stade de l'exécution. Les potentialités sont bien plus nombreuses dans les clauses d'exécution que dans les procédures de passation.

Des mesures comme le *Buy European Act* pourront s'avérer utiles, mais elles ne résoudront pas tout. Les mesures telles que l'assouplissement des procédures de passation, le relèvement des seuils et le motif d'intérêt général supposent que les acheteurs publics s'approprient ces outils. Or, la mise en œuvre des possibilités du code de la commande publique suscite des craintes, en particulier le délit de favoritisme. Par conséquent, alors même que ce n'est pas obligatoire, les acheteurs ont tendance à mener des appels d'offres ouverts. Il est sans doute nécessaire d'éduquer les acheteurs publics dans ce domaine. Par ailleurs, le *sourcing*, qui permet aux opérateurs informatiques de présenter leurs savoir-faire, devrait être davantage encouragé. Un autre levier important est l'allotissement, qui permet de confier aux entreprises de petite taille et aux opérateurs une partie des programmes. La difficulté est qu'en ce cas, l'interface doit être réalisée par la maîtrise d'ouvrage informatique. Or, les interfaces peuvent devenir très difficiles à gérer lorsque les deux prestataires sont en retard et se rejettent la faute mutuellement. Cela met même certains programmes à l'arrêt.

Il existe des solutions d'accompagnement pour faire émerger une offre, mais elles sont limitées. Si l'on examine maintenant l'aspect plus juridique de la souveraineté numérique, c'est-à-dire le respect des intérêts essentiels, des données sensibles ou la sécurité du traitement informatique, les leviers sont nombreux. Tout d'abord, les contraintes sont mieux admises en droit si elles sont légitimes. Comme cela a été rappelé, des dispositions du code de la commande publique permettent de protéger la sécurité informatique, de maintenir le traitement et le stockage des données sur place. D'une certaine manière, ces mesures peuvent même être « trop » efficaces. Par exemple, il est loisible aujourd'hui à un grand acheteur public d'exiger

des modalités d'accès aux codes sources et de maîtrise de ceux-ci, d'interdire le transfert des données numériques, de multiplier les clauses relatives à l'intégrité et à la confidentialité des données et même d'exiger des stipulations particulières relatives aux licences. Les géants américains proposent des offres très formatées, les contrats de licence sont très souvent imposés ou très faiblement négociables. Si vous considérez les stipulations du dossier de consultation des entreprises, le cahier des clauses administratives particulières (CCAP) ou le cahier des clauses techniques particulières (CCTP) l'emportent nécessairement sur toutes les offres des candidats, alors vous pouvez éliminer ces offres. Or, il est évident que les contrats de licence des géants ne sont pas fondamentalement négociables. Comment s'en sort-on aujourd'hui ? Les acheteurs publics ferment les yeux et l'on adopte la clause du CCAP relative à la hiérarchie des documents contractuels. Il y a d'abord le cahier des charges de l'administration, puis l'offre vient à la fin de la liste. Ainsi, l'offre du candidat ne l'emporte pas sur les besoins de l'administration. Le problème est que cette « rustine » cache en réalité un risque de non-conformité des offres. La clause n'est pas conçue pour couvrir la non-conformité, elle a vocation à traiter des incompatibilités tout à fait ponctuelles qui pourraient exister entre les stipulations de contrats très complexes. Face à un acheteur public qui peut imposer des clauses de propriété intellectuelle, de sécurité informatique, de stockage de données ou de non-transfert aux opérateurs économiques dans les appels d'offres au titre des contraintes d'exécution, de nombreux opérateurs n'accepteront jamais de négocier leur licence ou de renoncer à la possibilité de transférer des données aux États-Unis, lorsque le *Patriot Act* exige de la société mère le transfert des données détenues par les sociétés filiales. Par conséquent, si nous allons au bout de l'analyse, l'offre est irrecevable.

Des services de l'État ont été confrontés à ce problème. On leur a expliqué que dans un certain nombre de situations, les données fiscales devaient pouvoir être transmises à la maison mère parce que l'administration américaine le demandait. C'était cela ou ne pas avoir de prestataire. Les clauses existent aujourd'hui. Nous avons les moyens de la souveraineté numérique au stade des contraintes que nous pouvons imposer en termes d'exécution. Si nous le faisons, nous pourrons déclarer non-conformes aux besoins du pouvoir adjudicateurs les offres qui se présenteront, mais en ce cas, nous ne trouverons plus personne.

La Cour de justice a invalidé la décision de la Commission européenne qui estimait que les Américains respectaient rigoureusement la protection des données. Un arrêt du Conseil d'État belge a rappelé que les pouvoirs adjudicateurs n'étaient pas tenus de se soumettre au dispositif du RGPD, en ses articles 45 et 46, pour accepter le transfert des données : ce dernier peut être refusé. Nous avons aujourd'hui les moyens de la souveraineté numérique nationale en termes d'exécution. Nous pouvons faire respecter l'indépendance, la sécurité, l'intégrité et le non-transfert des données. Néanmoins, les pouvoirs adjudicateurs sont réticents à utiliser ces dispositifs, car ils n'ont alors plus d'offres. Dans les grands appels d'offres dont j'ai suivi la passation, on compte finalement peu d'offres crédibles. Par exemple, s'agissant du marché pour l'opérateur national de paye, un marché de 350 millions d'euros, nous avions au bout du compte une seule offre convenable. Il n'est pas rare qu'une seule offre soit crédible sur les grands marchés et elle n'est pas forcément nationale. Enfin, s'agissant du *Buy European Act*, une condition préalable sera de définir ce qu'est un opérateur économique national ou européen. Dès lors que des sociétés filiales sont admises à opérer librement en Europe et sur le territoire national, il est délicat de déterminer les opérateurs étrangers. Quels critères utilisera-t-on : la localisation du siège qui peut évoluer ? la détention du capital, qui peut être placé en bourse ? la nationalité des dirigeants, parmi lesquels on trouve toujours des Français ? Il est très difficile de décréter aujourd'hui quelles entreprises sont françaises. En somme, les enjeux et leviers de la souveraineté numérique sont dans l'exécution, mais nous devons être attentifs à défendre une politique de l'offre afin que les acheteurs publics trouvent des opérateurs qui présentent des offres crédibles.

M. Philippe Latombe, rapporteur. La CNIL a indiqué récemment qu'il n'était pas possible de recourir à des opérateurs concernant la partie RGPD, même s'ils étaient régulièrement domiciliés en Irlande. L'ensemble des GAFA sont localisés en Irlande et y ont un siège régulier, ce qui fait d'eux des acteurs européens. Dans ces conditions, comment les exclure ou prévoir de les intégrer différemment dans l'ensemble du champ légal de la commande publique ? Quels critères pourrait-on utiliser ? Par ailleurs, la localisation des serveurs est également un enjeu important, qu'il s'agisse du Health Data Hub ou de BPIfrance. Des acteurs disent avoir utilisé le *cloud* de Microsoft Azure ou d'AWS, qui donnent satisfaction. Ils invoquent l'absence de risque au motif que les clés de chiffrement sont chez nous et les serveurs localisés en Europe. S'il y a risque, comment s'en prémunir ? Les opérateurs peuvent-ils être écartés à ce titre ? Les acteurs du numérique sont très intéressés par ces sujets.

Pr Stéphane de La Rosa. Ces questions sont complexes, car elles se situent au croisement de deux logiques. La première est la liberté d'établissement et la caractérisation de l'établissement en droit européen. À ce sujet, les jurisprudences diffèrent selon les champs considérés. La deuxième est la logique propre à la commande publique. Les entreprises qui soumissionnent à des contrats de marché, informatiques ou autres, sont considérées comme des opérateurs économiques. Or, la notion d'opérateur économique est extrêmement large. N'importe quelle entité qui peut produire une offre et soumissionner à un contrat, sans être nécessairement une entreprise, est un opérateur économique. Par conséquent, toute entité publique ou privée, dès lors qu'elle est apte à faire une offre, peut se porter candidate indépendamment de sa localisation ou de son établissement. Ces critères n'apparaissent pas dans la définition des parties à un contrat de commande publique.

La nationalité des opérateurs des sociétés et de leurs filiales est une question également complexe. La jurisprudence a admis un certain nombre d'hypothèses de transfert de sièges sociaux et d'implantation de filiales par rapport à des sociétés mères. L'interface par rapport à la commande publique s'effectue essentiellement selon les conditions d'aptitude. Un acheteur peut invoquer les obligations d'enregistrement au registre du commerce et quant à l'immatriculation sociale et fiscale.

La question de l'abus de droit doit également être examinée avec attention. Face à certains montages fiscaux élaborés par les GAFA, la Cour européenne a ouvert la voie à des localisations qui seraient constitutives d'abus de droit, au terme du droit européen et du droit interne, en tant qu'elles visent à contourner les règlementations existantes. La qualification d'abus de droit devrait être mieux exploitée en matière de commande publique.

Enfin, la localisation et les transferts de données nous ramènent à une problématique de « bouclier ». Le risque est le transfert des données européennes aux États-Unis. La jurisprudence *Schrems* a donné lieu à plusieurs arrêts, dont le dernier de juillet 2020. Nous sommes confrontés à un enjeu de reconnaissance mutuelle : dans quelle mesure peut-on admettre qu'on a un système de protection à peu près équivalent chez des États tiers, en particulier aux États-Unis ? La question est très difficile, car par application du *Cloud Act* aux États-Unis, les renseignements américains exerceront toujours un contrôle sur les données qui doivent être transmises par les grandes entreprises. La Commission a soulevé récemment les autres questions de la cybersécurité et de la cyberdéfense. La révision des directives de cybersécurité des données et de cyberdéfense est différente du *Digital Act*. Elle constitue à mon avis un élément de réponse sur lequel le législateur français devrait prendre position.

M. François Benchendikh. C'est sans doute un vœu pieux de déterminer la qualification des entreprises, compte tenu de leur facilité à se déplacer sur le territoire de l'Union ou même mondialement. La notion d'entreprise locale ne comporte pas celle de

nationalité. Ainsi, une entreprise locale étrangère demeurerait une entreprise locale. Nous voyons cela illustré notamment dans un texte de 2017 sur les territoires ultramarins. Il est dit que l'on souhaite pouvoir privilégier une entreprise locale dans un appel d'offres. La commande publique peut faire office de levier pour permettre à certains territoires de bénéficier d'un achat public.

Je crois que l'intérêt général pourrait également être mobilisé dans ce cadre, bien qu'il ne soit pas en harmonie avec la directive européenne. Enfin, le centre de données *(data center)* public est un peu un serpent de mer. On s'est aperçu que des données de santé des collectivités étaient hébergées dans un État étranger. Les collectivités n'ont pas des informations suffisamment précises leur permettant d'avoir accès aux données. Je suis personnellement convaincu qu'il est nécessaire de développer un centre de données *(data center)* public. Une entité publique devrait être propriétaire des données. Ce peut être un syndicat mixte ou une structure juridique particulière, mais l'intérêt de ce système est que les données ne bougent pas après l'appel d'offres. Même si le gestionnaire est une entreprise informatique classique, les données demeureront localisées.

M. Philippe Latombe, rapporteur. Le logiciel libre est reconnu aujourd'hui comme pouvant être intégré dans des appels d'offres. Constitue-t-il une solution pour vous et si oui, comment concevez-vous sa mise en œuvre ? Le logiciel libre doit-il être privilégié comme le demandent un certain nombre d'acteurs du numérique, notamment français ? Comment percevez-vous son efficacité ?

Me Thierry Dal Farra. Un arrêt du Conseil d'État du 30 septembre 2011 redresse l'opinion d'un juge des référés précontractuels sur le fait qu'il est loisible à un pouvoir adjudicateur d'encourager des solutions de recours à des logiciels libres. La perspective est intéressante, mais soulève un certain nombre de difficultés. S'agissant de projets sensibles et de grande envergure, une solution à partir de logiciels libres n'offre pas de garanties de montée en version ou de mise à jour. En outre, quand vous téléchargez le logiciel libre, vous êtes tenus par la licence qui l'accompagne sans discussion possible. Celle-ci est rédigée en langue étrangère, les juridictions prévues sont également étrangères. Enfin, les responsabilités sont diluées : le logiciel étant libre, il n'est à personne et l'on ne trouve pas d'interlocuteur. L'utilisation du logiciel libre est envisageable pour des prestations standards à faible degré de sensibilité et pour autant qu'on puisse respecter les stipulations de la licence, mais ce point doit être examiné. Du point de vue du praticien, le logiciel libre n'est pas le remède miracle, notamment pour les grands projets sensibles, pour lesquels la souveraineté numérique est un enjeu essentiel.

Pr Stéphane de La Rosa. Je partage cette analyse. Il convient d'envisager l'usage du logiciel libre selon la taille, le montant du marché et le type de contrat, marché ou concession. Depuis quelques années, on observe quelques velléités contentieuses d'organismes représentant les logiciels libres qui viennent contester des appels d'offres au motif que les spécifications techniques désignent nommément un logiciel ou un exploitant plutôt qu'un autre, et méconnaissent par conséquent le principe d'égalité. Dans certains cas, il leur est donné raison. L'enjeu est que les spécifications techniques soient rédigées en termes strictement fonctionnels sans cibler un système d'exploitation ou un logiciel en particulier. Ce sont des organismes proches du logiciel libre qui ont déposé des recours concernant le Health Data Hub. Un référé du Conseil d'État du 13 octobre 2020 a enjoint de prendre des garanties supplémentaires face aux risque de transfert de certaines données.

Au-delà de l'aspect contentieux, s'agissant de la mise en œuvre, il est souhaitable de conduire une analyse fine de l'articulation entre les logiciels, les systèmes d'exploitation, l'obligation pour un système d'accueillir différents types de logiciels qui ne soient pas

incompatibles. De ce point de vue, le *Digital Act* obligerait les grands systèmes d'exploitation à accueillir des logiciels d'autres éditeurs.

M. François Benchendikh. Les éléments essentiels pour l'État ou les collectivités, lorsqu'ils s'engagent dans une relation contractuelle, sont les clauses du contrat. Elles peuvent notamment garantir les conditions d'utilisation, les conditions d'accès ou la capacité à se doter d'une *hotline*. Or, un logiciel libre ne permet pas ces garanties. L'élément fondamental lorsque l'État souhaite lancer un marché est la détermination préalable des besoins. C'est ce travail qui permettra à l'acheteur public de structurer le cahier des charges et de choisir l'entreprise la plus à même de répondre.

M. Philippe Latombe, rapporteur. Dans vos propos liminaires, vous avez tous évoqué l'éducation des acheteurs publics. Lorsque nous avons interrogé l'UGAP, la semaine dernière, ses représentants nous ont indiqué que leur activité de veille vis-à-vis des nouvelles solutions était très limitée. Avec des acheteurs qui ne sont pas parfaitement préparés, d'un côté, et une cellule de veille qui n'est pas à même de proposer des solutions très innovantes, de l'autre, on a tendance à adopter les mêmes solutions, le plus souvent intégrées et provenant des GAFA. Ce sont Microsoft 365 pour la gestion des mails, intégrant Azure, ou bien AWS pour BPI en ce qui concerne le prêt garanti par l'État (PGE). Comment inciter les acheteurs publics à prendre des risques, et dans quelles limites ? Comment procéder pour les éduquer ? Pourrait-on aller au-delà des observatoires ?

Me Thierry Dal Farra. En tant que praticien, je crois qu'il convient de distinguer la maîtrise des besoins et la maîtrise des procédures. S'agissant de la maîtrise des besoins, il existe en droit de la commande publique l'obligation de déterminer le besoin en amont de toute procédure de mise en concurrence. Cela suppose que l'acheteur public est omniscient. Or, vous ne pouvez commander que ce que vous connaissez. Nous sommes une nouvelle fois face à la logique de la demande qui est un peu antiéconomique, puisqu'en principe, c'est l'offre qui crée la demande. Si vous ne savez pas ce qui existe, vous ne pouvez pas le commander. Nous sommes donc face à un véritable problème, spécifiquement dans le domaine informatique, de non-maîtrise par les acheteurs publics de leurs propres besoins. Ils ne les maîtrisent pas parce qu'ils ne savent pas ce qui existe et ne savent pas quoi commander.

Il existe un certain nombre de techniques qui fonctionnement plus ou moins bien, telles que la méthode agile. Je considère qu'elles sont peu efficaces, car elles conduisent à contractualiser à nouveau après la passation du contrat. Elles peuvent également conduire à des contentieux d'exécution sans fin. Une technique permettant d'améliorer la maîtrise par les acheteurs publics de leurs propres besoins en matière d'informatique est d'encourager le *sourcing*, c'est-à-dire de permettre à des opérateurs économiques, en les encadrant davantage et sans favoritisme, de proposer des solutions qu'ils ont conçues. À un moment donné, lorsque la discussion s'arrête, on lance la procédure dans le respect du principe d'égalité. Quoi qu'il en soit, il est très important que les acheteurs publics maîtrisent mieux leurs besoins. La prise de risque n'est pas tolérable sur ce point, car faute de maîtrise, ce qu'ils commandent ne correspond pas à ce qu'ils obtiendront. Ils devront alors changer les besoins en cours d'exécution du contrat lorsqu'ils s'apercevront que ce qu'ils ont commandé ne correspond pas à la totalité de leurs besoins.

Le deuxième problème est la maîtrise des procédures. Prendre des risques est difficile lorsque toute la matière est pénalement sanctionnée. Quand vous examinez les arrêts de la Cour de cassation en matière de favoritisme, la moindre irrégularité est constitutive d'une infraction. Alors même qu'aux termes de l'article 432-14 du code pénal, le délit est constitué par le fait d'avoir procuré ou tenté de procurer un avantage à autrui par violation des règles garantissant l'égalité et la liberté d'accès aux contrats de la commande publique, la Cour de

cassation a complètement « écrasé » la première condition sur la tentative ou l'octroi d'un avantage injustifié. Elle considère que toute violation des règles de passation induit obligatoirement un avantage injustifié. L'écrasement de la première condition entraîne un élargissement du champ du délit. De fait, la moindre irrégularité peut conduire au délit de favoritisme. J'ai soulevé une question prioritaire de constitutionnalité concernant l'écrasement de la condition tenant à l'avantage injustifié, mais il est peu concevable qu'un acheteur public prenne un risque, alors qu'on lui explique que, s'il commet la moindre irrégularité, il risque de tomber sous l'accusation de favoritisme.

Même dans les marchés à procédure adaptée, les acheteurs ne bénéficient pas de la liberté que le code leur octroie. Alors qu'ils pourraient rencontrer les opérateurs, afin d'éviter les risques, ils font de l'appel d'offres ouvert, car c'est la voie la plus commode. Quant à l'UGAP, elle fonctionne bien pour les fournitures standards, mais elle n'est pas le bon instrument pour les solutions innovantes, car ils ne connaissent pas forcément tous les besoins de leurs clients. À mon sens, la meilleure perspective pour maîtriser les besoins consiste à encourager une meilleure connaissance de l'offre par le *sourcing*.

Pr Stéphane de La Rosa. En ce qui concerne l'accompagnement des acheteurs, les formations proposées dans les universités demeurent très juridiques. Il s'agit de formations classiques en droit des contrats. Il me semble que la technique de l'acheteur public est insuffisamment investie. Il est important que la formation des futurs juristes en commande publique ne se limite pas aux aspects juridiques et contentieux. Cette évolution est d'autant plus nécessaire que lorsque nous examinons nos voisins, l'approche est différente. Par exemple, aux États-Unis, les juristes en commande publique sont formés de manière beaucoup plus concrète.

La question du *sourcing* est essentielle. Les acheteurs publics sont toujours réticents à en faire usage. Il y a dix ans, on attribuait le contrat à la personne qui avait défini le besoin. Cette technique a été condamnée par la Cour de justice. La compréhension du *sourcing* doit être affinée. La mise en place d'un portail public d'accès à l'offre existante serait un moyen d'approfondir les connaissances des acheteurs dans ce domaine. Le travail sur ce point est insuffisant, tant en France qu'au niveau de la Commission ou des autres institutions européennes. Si la Commission produit régulièrement des communications un peu techniques sur les bonnes pratiques observées ici ou là, elle ne propose pas de portail global de l'offre européenne d'entreprises numériques. Un travail pourrait être conduit pour développer la connaissance de l'offre, détaillant notamment les systèmes d'exploitation ou les aspects relatifs à la cybersécurité.

Enfin, la question des marchés de R&D sur les solutions innovantes doit être approfondie. En l'état actuel du droit, les marchés de R&D échappent au code. On peut attribuer un marché de R&D sans s'y soumettre. Le problème est que ces marchés doivent être uniquement à des fins d'établissement de prototypes. En d'autres termes, ils ne peuvent pas avoir de prolongement industriel. Quel est l'intérêt pour un opérateur de développer ce type de marché s'il ne peut pas l'exploiter d'un point de vue commercial ? L'outil est sans doute intéressant, mais il doit évoluer afin de donner une viabilité économique réelle aux projets financés en R&D.

François Benchendikh. Un autre élément important est le cadre d'emploi. Une personne qui détient des connaissances assez poussées en informatique, si elle souhaite une rémunération attractive, aura tendance à rejoindre le privé plutôt qu'une collectivité ou l'État. L'enjeu pour l'acheteur public est de compter chez lui un ingénieur informatique qui privilégierait une carrière publique. La difficulté à faire émerger des projets est cependant fondamentale : des collectivités ou certains services de l'État ne savent pas ce qu'ils

souhaiteraient, parce qu'ils ne peuvent connaître avec précision leurs besoins. Certains pourront solliciter un bureau d'études, mais la démarche demeure compliquée. Sur les marchés téléphoniques, par exemple, les collectivités dépensent des sommes colossales parce que les offres ne leur sont pas adaptées.

En ce qui concerne l'élaboration du portail, les données sont disponibles. Avec l'aide des chambres consulaires et de certains syndicats patronaux, le portail pourrait faciliter largement les projets et permettre l'avènement du *sourcing*.

M. Philippe Latombe, rapporteur. Y a-t-il des sujets que nous n'aurions pas encore abordés ? Souhaitez-vous encore apporter d'autres précisions ?

Pr Stéphane de La Rosa. À titre conclusif, il me semble que votre mission appelle une clarification de la notion de souveraineté numérique. Le volet interne et stratégique consiste à privilégier les entreprises françaises afin de compter des champions nationaux. Le volet externe consiste à organiser une défense efficace contre des comportements prédateurs ou des pratiques déloyales. La question de la souveraineté se pose aussi dans un cadre européen, dans la mesure où les normes sont aussi européennes. Ces aspects doivent être pensés ensemble, afin d'obtenir une compréhension fine de la souveraineté numérique et de ne pas en faire un « attrape-tout ».

Deuxièmement, il est important d'adopter une nouvelle position par rapport à l'accord sur les marchés publics. Les calculs des seuils nous viennent de l'AMP, ainsi que les clauses de non-discrimination par rapport aux États tiers. En outre, dans la hiérarchie des normes européennes, l'AMP prévaut sur les directives européennes. Or, on est confronté à une tendance à questionner le contenu de l'AMP, en particulier aux États-Unis. Il serait donc important que la France tienne un discours clair sur l'AMP. Doit-on le renégocier, émettre des réserves ? Si ce travail n'est pas effectué, la souveraineté numérique ne sera pas bien définie sur le plan technique et juridique. Enfin, une réflexion doit être menée sur les grands financements publics. Il convient d'envisager l'évolution du droit des aides d'État en ce qui concerne le financement de projets innovants. Ces approches doivent s'inscrire dans une perspective plus large qui est le marché numérique et la réorientation de la politique industrielle européenne.

M. Philippe Latombe, rapporteur. Nous avons commencé notre mission par un travail de définition de la souveraineté numérique afin d'éviter les acceptions trop générales. Selon vous, une réflexion est-elle en cours sur l'AMP à l'heure actuelle ?

Pr Stéphane de La Rosa. Comme l'atteste le décret de Joseph Biden publié depuis quelques jours, la réflexion est engagée aux États-Unis. L'administration américaine vise un repositionnement de l'AMP afin de proposer un système d'offre. S'agissant de la Commission, je ne peux vous répondre avec précision. Quoi qu'il en soit, les mécanismes de préférence et de *Buy European Act* me semblent indissociables d'une réflexion sur le texte.

Me Thierry Dal Farra. Je souscris à ce qui vient d'être dit : il n'y aura pas d'évolution significative sans un accompagnement européen. Il est très important de développer une politique de l'offre à laquelle l'acheteur public puisse contribuer, car, afin d'acheter européen, encore faut-il qu'une offre européenne existe. De même, afin d'acheter français, l'offre économique la plus avantageuse doit être l'offre nationale. Nous avons aujourd'hui les moyens d'exclure du champ les géants américains en alléguant des clauses incompatibles avec leurs politiques de groupe. Mais si nous n'avons pas entre temps contribué à l'élaboration d'une offre alternative, nous n'aurons personne. En somme, le risque est soit de n'avoir que des offres irrégulières, soit de ne pas avoir d'offres. Les grands acheteurs publics français que je

connais ont pour objectif premier de satisfaire les besoins et d'assurer le bon fonctionnement des services publics. Ils sont par conséquent portés à choisir l'offre la plus efficace.

Au-delà des aides d'État, plusieurs pistes peuvent être proposées pour développer la politique d'offre numérique. La première est le *sourcing* qui permettrait une meilleure connaissance des solutions innovantes françaises. La deuxième est l'élaboration de participations de l'État à des entreprises. L'État pourrait être présent le temps de créer l'offre et ressortir ensuite. Il aurait alors contribué à bâtir une filière. Cela s'est fait dans le domaine de l'énergie dans les années 1970. Pourquoi ne pas l'envisager dans les années 2020 pour le numérique ? L'importance de l'enjeu le justifie.

M. François Benchendikh. Il est nécessaire de développer une recherche publique fondamentale sur la question numérique. Elle pourrait contribuer à l'émergence d'entreprises et d'acteurs qui en bénéficieraient. Un autre élément important est la place et le rôle des services de l'État, qu'il s'agisse de l'agence du numérique ou de la DINUM. Chaque direction peut permettre de trouver des solutions.

Audition commune de Mme Laure Bédier, conseiller d'État, directrice des affaires juridiques au ministère de l'Économie et des Finances, agent judiciaire de l'État, et de M. Benoît Dingremont, administrateur civil au ministère de l'Économie et des Finances
(28 janvier 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Notre mission d'information achève aujourd'hui son cycle d'auditions consacrées à la commande publique. À cette étape de nos réflexions, il nous semble important de faire le point sur le champ des possibles dans ce domaine, dans l'objectif de protéger et de promouvoir notre souveraineté numérique aux niveaux national et européen.

M. Philippe Latombe, rapporteur. Je souhaiterais évoquer trois sujets. Tout d'abord, pourriez-vous nous présenter à grands traits un état des lieux du droit de la commande publique et ses principales évolutions ces dernières années ? Un certain nombre d'initiatives ont été prises pour moderniser la commande publique. Je pense à la fois au plan de transformation numérique engagé pour la période 2017-2022, à la loi d'accélération et de simplification de l'action publique du 7 décembre 2020 (loi ASAP), et aux mesures pour encourager le recours à davantage de solutions innovantes, *via* l'expérimentation d'un dispositif dédié depuis 2018. J'aimerais connaître votre regard sur ces éléments et prendre connaissance à cette occasion des travaux de l'observatoire économique de la commande publique qui pourrait éclairer notre démarche. En second lieu, quelles sont, selon vous, les évolutions envisageables ou souhaitables du droit de la commande publique afin de promouvoir par son truchement notre souveraineté numérique ? J'aimerais en particulier savoir s'il existe déjà des outils permettant de favoriser l'achat par des acteurs publics de matériel et de logiciels souverains. Si tel n'est pas le cas, quelles devraient être les caractéristiques d'un nouveau régime juridique allant dans ce sens, en conformité avec le droit européen ? Nous sommes ouverts à toutes vos propositions sur ce sujet. Elles nous permettront notamment de faire le lien avec l'audition précédente, au cours de laquelle des professionnels du droit ont émis quelques suggestions. Enfin, j'aimerais vous interroger plus globalement quant à l'influence des règles actuelles de la commande publique sur la capacité des acheteurs publics à prendre des risques dans leurs pratiques d'achats. La semaine dernière, si M. Nadi Bou Hanna, directeur interministériel du numérique, nous a indiqué que le code de la commande publique pouvait être « désincitatif » sur ce point, la direction des achats de l'État ne semblait pas tout à fait en accord. Quelle est votre position à cet égard ? Des modifications sont-elles envisageables pour lever les obstacles qui semblent exister sur ce sujet ?

Mme Laure Bédier, conseiller d'État, directrice des affaires juridiques au ministère de l'Économie et des Finances, agent judiciaire de l'État. La direction des affaires juridiques se compose de quatre sous-directions, dont la sous-direction du droit de la commande publique, représentée par M. Benoît Dingremont aujourd'hui. Cette sous-direction est en charge de l'élaboration du droit de la commande publique et de la norme. Elle propose également du conseil aux acheteurs, elle élabore à leur attention des fiches de doctrine. Elle s'occupe également du recensement des statistiques de la commande publique et elle publie des guides. Cette dernière activité s'exerce dans le cadre de l'observatoire économique de la commande publique (OECP), qui a remplacé en 2016 l'observatoire économique de l'achat public. L'objectif était d'aller au-delà des marchés publics et d'intégrer les concessions. L'observatoire économique de la commande publique est organisé autour d'une assemblée

plénière qui décide de ses travaux et qui rassemble les parties prenantes de la commande publique, c'est-à-dire, à la fois, des acheteurs et des opérateurs économiques. L'assemblée plénière n'a pu se tenir cette année, mais cela n'a pas empêché l'observatoire économique de la commande publique de publier deux guides qui ont été largement téléchargés par les acheteurs et par les entreprises. Le premier guide porte sur l'accès des TPE/PME à la commande publique. Le deuxième concerne l'achat innovant. Pour 2020, nous avons publié un document sur la sous-traitance qui n'est pas sans lien avec vos travaux. En 2021, nous travaillerons sur les concessions et sur leurs aspects statistiques. Les États membres sont obligés d'adresser tous les trois ans un rapport à la Commission sur la règlementation et son application en matière de commande publique. La sous-direction du droit de la commande publique suit enfin les questions relatives à la transition numérique de la commande publique.

La deuxième sous-direction qui compose notre direction est la sous-direction du droit privé et du droit pénal, qui exerce des missions de conseil et d'expertise dans ces secteurs et qui gère les dossiers de l'agent judiciaire de l'État. Ce dernier a le monopole de la défense des intérêts de l'État, lorsqu'il s'agit d'intérêts financiers, à la fois en demande et en défense, devant les juridictions judiciaires. Nous comptons environ 11 000 dossiers. La sous-direction du droit public et du droit européen international donne des conseils dans ces domaines. Enfin, la sous-direction du droit des régulations économiques traite du droit financier, du droit des assurances, du droit des entreprises et donne des conseils dans le domaine du numérique pour la protection des données personnelles. Je précise que nous sommes une direction de conseil et non une direction opérationnelle. Nous n'effectuons donc pas d'achats. C'est la direction des achats de l'État (DAE) qui exerce la pratique des achats publics.

Voici maintenant quelques chiffres concernant la commande publique. En 2019, nous avons enregistré 170 000 marchés pour un montant d'un peu plus de 110 milliards d'euros. Les PME représentent plus de 60 % du total en nombre et 30 % en montant. La répartition entre fournitures et travaux est variable. Par exemple, l'État et les établissements hospitaliers ont beaucoup plus de fournitures. Ces dernières représentent près de 50 % du montant. À l'inverse, les collectivités territoriales dépensent davantage en travaux. Plus de 20 % des marchés sont supérieurs au seuil européen et ils représentent un montant très important.

Les marchés numériques au sens large représentent un montant de 5,3 milliards d'euros, qui se répartit en 2 milliards d'euros pour l'État, dont 500 millions d'euros pour les armées, et 500 millions d'euros pour les collectivités territoriales. Les autres acheteurs, qui représentent environ 3 milliards d'euros, sont essentiellement les opérateurs de réseaux. L'acteur le plus important sur ce marché est la SNCF, qui représente 800 millions d'euros, EDF représentant 700 millions d'euros.

S'agissant de la souveraineté numérique nationale et européenne, notre droit est assez contraint, car, si l'on excepte les marchés de défense et de sécurité, pour lesquels nous pouvons faire valoir une préférence européenne, les outils permettant de défendre la préférence sont très limités. Je les cite rapidement pour les écarter, car ils ne sont pas applicables aux marchés informatiques. Le premier est la possibilité de déroger aux procédures de publicité et de mise en concurrence en cas de menace grave. Nous ne nous inscrivons évidemment pas dans ce cadre. Le deuxième est l'article 52 du Traité sur le fonctionnement de l'Union européenne (TFUE) qui permet de déroger, pour des raisons d'ordre public et de sécurité publique, à un certain nombre de principes européens, notamment la liberté d'établissement. Le problème est qu'un argument économique n'est pas suffisant pour déroger aux principes applicables au sein de l'Union européenne. Néanmoins, cet article peut être une piste de développement d'autres outils. L'État a engagé des réflexions sur l'instauration d'un *cloud* souverain sur la base de l'article 52. Pour le reste, nous sommes très encadrés par l'accord sur les marchés publics

(AMP), parce que contrairement aux États-Unis qui ont négocié un *Buy American Act*, l'Union européenne n'a pas négocié ce dispositif et ne peut défendre une préférence européenne.

Il existe néanmoins au sein des directives deux articles qui nous permettent de restreindre un peu l'accès des pays tiers aux marchés européens. Le premier est l'article 85 de la directive de 2014, qui a été transposé à l'article L. 2153-2 du code de la commande publique. Il permet d'écarter les offres qui se composent à plus de 50 % de produits provenant d'États tiers à l'Union européenne. Les États tiers sont les États qui n'ont pas signé l'AMP ou qui n'ont pas signé de traités commerciaux bilatéraux avec l'Union européenne. Cet article n'est pas d'application aisée. Tout d'abord, il ne s'applique qu'aux opérateurs de réseaux, c'est-à-dire aux domaines de l'eau, de l'énergie et des transports. Ensuite, il ne s'applique qu'aux marchés de fournitures. Si le marché est à la fois un marché de services et de fournitures, l'article 85 n'est pas applicable. En outre, il est complexe à mettre en œuvre, car il est très difficile de déterminer l'origine du produit, qui diffère selon les États de l'Union européenne. Il suffit donc d'entrer dans un pays peu regardant pour être considéré comme européen à plus de 50 %. Nous avons tenté de clarifier la situation en publiant récemment une fiche sur l'application de l'article 85.

Par ailleurs, nous avons interprété *a contrario* l'article 25 de la directive pour introduire dans la code de la commande publique l'article L. 2153-1, qui permet d'écarter une offre d'une entreprise issue d'un État tiers. Cet article n'est pas simple à appliquer non plus, notamment parce qu'il est difficile de déterminer le champ exact couvert par l'accord sur les marchés publics et les traités bilatéraux. S'agissant de l'accord sur les marchés publics, chaque pays peut émettre ce que l'on appelle une offre de couverture : il n'adhère pas à l'ensemble de l'AMP, mais il choisit les secteurs pour lesquels il adhère. Il est par conséquent compliqué de savoir ce qui est couvert par l'accord. Par ailleurs, cet article ne s'applique qu'aux offres provenant d'entreprises situées dans des États tiers et ne s'applique donc pas lorsqu'il existe une filiale en France ou en Europe. Or, l'entreprise soumissionnaire compte très souvent un établissement en France ou en Europe. Elle ne peut donc être écartée au seul motif qu'elle appartient à un groupe étranger. Le pourcentage de marchés publics attribués à des entreprises étrangères est très faible, de l'ordre de 2 à 3 %, ce qui est assez contre-intuitif, mais dans de nombreux cas, elles comptent des filiales françaises. La dernière fragilité de ce dispositif est qu'il s'agit d'une interprétation *a contrario* dans le domaine des négociations commerciales, qui est un domaine exclusif de la Commission.

Dans le groupe de travail « marchés publics », nous tentons d'obtenir de l'Union européenne des avancées sur ces sujets et en particulier une modification des directives, et ce, à plusieurs fins. Premièrement, nous souhaiterions clarifier ce qui peut être fait dans le cadre de l'article 25 de la directive 2014, tel que transposé. Il serait souhaitable que l'Union européenne puisse aider ses membres à déterminer la liste des pays et des produits couverts par les accords commerciaux, afin de savoir avec précision dans quels cas une offre d'État tiers peut être écartée. Un autre objectif est de clarifier l'application de l'article 85 qui comporte la notion de produit d'origine et d'étendre cet article à l'ensemble des acteurs, au-delà des opérateurs de réseaux. L'enjeu est de travailler dans le cadre des directives, parce que s'engager dans une renégociation de l'accord sur les marchés publics semble très compliqué. La France est assez isolée sur ce sujet complexe. Il est plus efficace d'utiliser l'ensemble des possibilités offertes par les directives pour favoriser les offres européennes dans les secteurs stratégiques.

Cela étant, en dehors de cette action, le code de la commande publique comporte des outils qui nous permettent de tenter de privilégier l'offre européenne. Comme nous le rappelons souvent dans les fiches que nous publions, le *sourcing* est un élément essentiel. Il

est très important de connaître l'offre nationale pour pouvoir adapter la demande en conséquence. L'allotissement permet aux petites entreprises nationales d'accéder aux marchés publics. Il est par ailleurs important de choisir des critères qui ne soient pas seulement liés aux prix, mais qui concernent également la qualité. Par exemple, on parle souvent du critère environnemental. Les critères doivent être pondérés de manière à ce que le prix ne soit pas le seul élément pris en compte dans la sélection. Il est également possible d'établir des clauses d'exécution sur la sécurité et l'intégrité des données. On recommande également de porter une grande attention à l'application du RGPD. Il n'est pas possible de rejeter une candidature au seul motif que l'entreprise est soumise au *Cloud Act* américain. En d'autres termes, le droit de la commande publique ne permet pas de rejeter une candidature parce qu'une entreprise pourrait ne pas respecter les règles nationales et européennes. Nous pouvons toutefois maximiser les chances des entreprises européennes en rappelant la nécessité de respecter le RGPD. Par exemple, lorsque des données présentent un caractère sensible, on peut exiger leur stockage en Europe et interdire le contrôle des données depuis un groupe installé hors du territoire européen. On peut également prévoir de sanctionner la transmission des données à caractère personnel, y compris si elle est censée s'effectuer en application d'une législation étrangère. On peut enfin faire de toutes ces garanties un critère de classement.

Nous sommes en train de mener un travail sur les cahiers des clauses administratives générales (CCAG). Bien que ces documents ne soient pas obligatoires, les acheteurs y recourent très fréquemment. Dans une révision assez générale de ces CCAG, qui seront publiés au mois d'avril, un certain nombre de travaux ont porté sur la protection des données personnelles. Nous proposons d'insérer dans l'ensemble des CCAG des dispositions rappelant les règles du RGPD. Nous proposons en outre de prévoir une obligation de déclaration informant l'acheteur en cas de recours à un sous-traitant pour la mise en œuvre du traitement de données. Nous proposons aussi une obligation d'informer l'acheteur de toutes les mesures lui permettant de s'opposer à des transmissions de données qui seraient contraires à la réglementation européenne. Nous proposons enfin de prévoir des pénalités en cas de violation de la protection des données. La révision des CCAG vise en somme à renforcer la protection des données personnelles.

Vous avez évoqué les achats innovants. Il s'agit d'une expérimentation qui date de décembre 2018, permettant de dispenser de publicité de mise en concurrence les achats de produits innovants au-dessous de 100 000 euros jusqu'au 24 décembre 2021. Nous devrions obtenir un bilan de cette expérimentation au mois de juin. Au 1er janvier, 174 marchés ont été déclarés auprès de l'OECP pour un total de 11 millions d'euros, très probablement sous-estimé. De manière générale, les acheteurs déclarent assez peu leur marché à l'OECP et les achats innovants sont compliqués à déclarer. Les premiers résultats fournissent néanmoins un bon aperçu du dispositif. Il est utilisé principalement, à près de 60 %, pour les marchés de services. La moitié de ces marchés portent sur des montants supérieurs à 75 000 euros et les marchés informatiques ne représentent qu'un tiers de ces marchés innovants. De nombreux marchés concernent l'achat responsable, c'est-à-dire l'innovation sociale et environnementale, ainsi que l'économie circulaire.

Afin de favoriser le recours à ce dispositif, nous avons publié un guide définissant un faisceau d'indices qui permettent de qualifier un achat d'innovant. Le principal frein au recours à ce dispositif est l'incertitude autour de la notion d'achat innovant. Il importe de savoir si l'on se trouve dans un cadre qui permet de se dispenser de publicité et de mise en concurrence. Il n'est pas certain que ce soit suffisant, mais c'est tout ce que nous avons pu faire à notre niveau. Le guide ayant été largement téléchargé, nous espérons qu'il aura aidé les acheteurs à s'emparer de ce dispositif, même si les chiffres que je cite sont, pour l'heure, un peu décevants.

Dans la réglementation nationale récente, la loi ASAP a été adoptée dans un objectif de simplification des procédures et de soutien à l'économie. La mesure phare, qui n'est pas forcément très applicable aux marchés numériques, est la dispense de publicité et de mise en concurrence pour les marchés de travaux, en-dessous de 100 000 euros, jusqu'au 31 décembre 2022. La loi pérennise aussi un certain nombre de mesures prises pendant l'état d'urgence sanitaire. Elle rappelle notamment que les entreprises en redressement judiciaire bénéficiant d'un plan de redressement peuvent soumissionner aux marchés publics. Le Conseil d'État l'avait dit, mais cette possibilité demeure peu connue des acheteurs. Des dispositions permettent également de réserver, pour les marchés globaux, des parts aux TPE/PME.

Une autre mesure, qui a été très mal comprise, permet, pour un motif d'intérêt général, de se dispenser de recourir à la publicité et à la mise en concurrence. Elle a été mal comprise tout d'abord parce qu'elle ne s'applique qu'en-dessous des seuils européens. Au-dessus de ces seuils, on s'inscrit, par définition, dans le cadre des règles européennes de publicité et de mise en concurrence. L'idée n'est pas de permettre à un acheteur considérant qu'il a un motif d'intérêt général de se dispenser des formalités de publicité et de mise en concurrence. La disposition vise plutôt à fournir une base législative à des mesures règlementaires de dérogation de publicité et de mise en concurrence qui seront prises par décret en Conseil d'État, avec un contrôle strict de ce dernier. Par exemple, si l'on pérennise la disposition de l'achat innovant afin de soutenir l'écosystème des start-up nationales, l'intérêt général du soutien aux start-up permettra de justifier la dérogation au seuil de publicité et de mise en concurrence. La mesure doit s'appliquer à des secteurs très précis, de manière limitée et sous le contrôle du Conseil d'État. Par conséquent, le champ d'application de cette mesure demeure très limité.

Le plan de transformation numérique de la commande publique court sur cinq ans, de 2018 à 2022. Il associe la direction des affaires juridiques, la direction des achats de l'État et l'agence pour l'informatique financière de l'État. Il a bénéficié d'un soutien du fonds de transition numérique de l'action publique. L'objectif du plan est de dématérialiser, de bout en bout, les différentes étapes de la commande publique. Nous avons conduit une dématérialisation de la passation des marchés publics en octobre 2018. Il s'agissait d'une obligation européenne, que nous avons appliquée en dessous des seuils européens. Le projet est de dématérialiser la suite de la chaîne de la commande publique, et notamment l'exécution des marchés publics. Afin d'atteindre cet objectif ambitieux, nous essayons de développer l'interopérabilité entre les systèmes d'information, et surtout la création de briques en *open source* qui pourront être implémentées sur les plateformes des acheteurs, qu'on appelle les profils d'acheteurs. Le projet se construit autour de la plateforme d'achat de l'État. On y associe un certain nombre d'importantes plateformes d'acheteurs, Maximilien pour l'Ile-de-France et Mégalis pour la Bretagne. L'enjeu est de faire croître à une taille critique les plateformes qui utilisent ces briques en *open source*, afin qu'elles puissent se diffuser vers l'ensemble des acheteurs publics.

Jusqu'en 2020, nous avons surtout travaillé sur le socle du projet, c'est-à-dire le cadre commun d'urbanisation et la cartographie des SI. Le projet n'est donc pas encore très visible de l'extérieur. À compter de l'année prochaine, nous pourrons offrir des services permettant de favoriser la dématérialisation, tels que la signature électronique ou la transmission des avis de publicité. Les avis de publicité seront regroupés sur un portail, ce qui permettra aux entreprises de les consulter en un lieu unique. Le projet a pris un peu de retard en raison du COVID, mais il se poursuit et nous devrions pouvoir offrir un certain nombre de briques aux acheteurs en 2022, leur permettant de dématérialiser de bout en bout la commande publique.

J'évoquerai pour terminer la prise de risque que vous avez mentionnée en introduction. Il est certain que la commande publique est une opération très complexe. Cela ne tient pas au droit national, mais au droit européen. Lors de la transposition des directives, nous avons donc tenté de porter le souci de simplification au niveau européen. Nous continuerons de défendre ce besoin, mais nous sommes très encadrés par le droit européen. Nous avons adopté, au cours des dernières années, plusieurs mesures destinées à favoriser cette simplification. Je ne suis pas certaine que nous puissions aller plus loin. Il convient à présent d'utiliser les outils existants. Il est donc important de bien communiquer sur ce que permet le code de la commande publique.

M. Philippe Latombe, rapporteur. La vision de l'AMP pourrait-elle évoluer avec le décret du président Joseph Biden du 25 janvier, relatif au *Buy American Act* ? Il y est indiqué que les États-Unis souhaiteraient renégocier l'AMP. N'est-ce pas une opportunité que l'Europe et la France devraient également saisir ? S'agissant des risques, un juriste a expliqué, durant l'audition précédente, que la Cour de cassation retient une jurisprudence peut-être trop stricte, en considérant que la moindre infraction entraîne un délit de favoritisme, sans prendre en compte l'intentionnalité. Il en résulte une approche très prudente des acheteurs publics qui les empêche de prendre des initiatives et de s'orienter vers du *sourcing*. Partagez-vous cette appréciation ? Des évolutions législatives sont-elles envisageables pour redonner un peu de souplesse à ce dispositif ? Enfin, quand le décret en Conseil d'État auquel vous faisiez allusion pourrait-il paraître ? Son champ d'application s'étendra-t-il aux logiciels et aux infrastructures informatiques-numériques ?

Mme Laure Bédier. Ce n'est pas la direction des affaires juridiques qui mène les négociations au niveau européen, y compris sur les directives que j'ai évoquées. C'est surtout la direction générale du Trésor qui porte ces négociations. Néanmoins, il me semble que la crise sanitaire est une opportunité d'examiner la possibilité d'établir un *Buy European Act*. Or, il m'a été indiqué que même ces circonstances, qui accroissent la difficulté de ne pas pouvoir favoriser des entreprises nationales pour des raisons de sécurité d'approvisionnement, ne sont pas suffisantes pour faire évoluer les membres de l'Union européenne sur ce sujet et faire avancer la Commission. Je ne sais pas si le décret signé par le président Joseph Biden et le *Buy American Act* seront un élément suffisant.

Le délit de favoritisme est un véritable problème. La Cour de cassation en fait un délit objectif, ce qui signifie qu'on n'a plus besoin de prouver l'intention de vouloir violer les règles des marchés publics. Ce risque tétanise effectivement les acheteurs. La crainte est peut-être quelque peu infondée dans la mesure où, en pratique, les condamnations pour délit de favoritisme ne sont pas fréquentes. Néanmoins, la conjonction d'une incertitude concernant les modalités d'application, d'une part, et d'une jurisprudence qui caractérise un délit à la moindre infraction aux règles de la commande publique, d'autre part, paralyse les acheteurs. L'infraction étant assez « politique », commencer à réduire son champ d'application pourrait soulever un certain nombre de difficultés.

M. Philippe Latombe, rapporteur. Comment pourrait-on faire pour lever ce frein ? Devrait-on réécrire l'article en question ?

Mme Laure Bédier. Oui. On a déjà tenté à plusieurs reprises de réécrire cet article pour tenter de restreindre le délit de favoritisme au délit intentionnel, mais ces tentatives de réforme soulèvent chaque fois une opposition.

Je reviens à la disposition ASAP, car je n'ai pas été parfaitement claire à ce sujet. Elle consistait à introduire la notion d'intérêt général, à côté de celle d'intérêt de l'acheteur, dans la partie législative du code de la commande publique qui énumère les cas dans lesquels on

peut se dispenser de publicité de mise en concurrence. Jusqu'à présent, toutes les dérogations prises par décret pouvaient se justifier par l'intérêt de l'acheteur, mais certaines dispositions étaient assez fragiles. Par exemple, la dispense de publicité et de mise en concurrence pour l'achat de livres scolaires en-dessous de 90 000 euros relève plutôt de l'intérêt général que de l'intérêt de l'acheteur. Notre préoccupation était d'introduire dans la partie législative une disposition qui sécurisât l'ensemble des dérogations actuelles et qui nous permît le cas échéant d'en établir d'autres. Si je reprends l'exemple de l'achat innovant, il relève à la fois de l'intérêt de l'acheteur et de l'intérêt général, l'enjeu étant de favoriser l'innovation en France. À cette fin, nous avons introduit l'intérêt général dans la partie législative du code de la commande publique. S'il n'est pas question de définir la notion d'intérêt général par décret, nous pourrions édicter un décret pour un secteur particulier, souvent pour une durée limitée, et sous le contrôle du Conseil d'État qui jugera du caractère proportionné de l'intérêt général par rapport à la mesure proposée.

M. Philippe Latombe, rapporteur. Pensez-vous qu'en application de cette disposition législative, il faille reprendre le décret sur la partie achat innovant ?

Mme Laure Bédier. Nous dresserons en fin d'année le bilan de ce dispositif. Pour l'instant, les acheteurs sont favorables à sa pérennisation. La disposition législative sur l'intérêt général nous permettra de prendre un décret pérennisant la dispense à 100 000 euros pour l'achat innovant.

M. Benoît Dingremont, sous-directeur en charge de la commande publique au sein du ministère de l'Économie et des Finances. L'accord sur les marchés publics est complexe et il soulève de nombreuses incompréhensions et difficultés de communication. Vous avez relevé à juste titre les propositions du nouveau président américain. J'ai compris qu'il engageait dès maintenant pour les marchés fédéraux des États-Unis l'application pleine et entière du *Buy American Act*. On a beaucoup de mal à expliquer pourquoi les Américains, qui sont partie à cet accord, peuvent prendre cette initiative, alors que les Européens ne le peuvent pas. Cela tient en réalité au caractère, non multilatéral, mais plurilatéral de l'AMP. S'agissant d'un accord multilatéral, les mêmes obligations s'appliquent intégralement à toutes les parties. Dans l'accord plurilatéral, si les principes sont communs à tout le monde, ils s'additionnent d'offres de couverture, correspondant à ce que chaque partie s'engage à ouvrir à la concurrence internationale. Ces offres de couverture ne sont pas rédigées de façon identique, mais les parties considèrent qu'elles sont équivalentes. Dès 1994, les Américains ont placé dans leur offre de couverture une réserve précisant que, dans certains secteurs, il était possible de réserver une partie des marchés américains aux entreprises américaines, et notamment aux PME américaines. C'est ce que le président américain souhaite faire appliquer pleinement, plutôt que de rouvrir des négociations AMP, au cours desquelles les Européens pourraient tenter d'obtenir quelque chose d'équivalent.

En ce qui concerne les CCAG, le *Cloud Act* permet aux juges américains et à l'administration américaine de demander aux entreprises américaines et aux filiales étrangères de ces entreprises de leur communiquer des données dans un certain nombre d'enquêtes, terroristes ou de sécurité notamment. Par conséquent, des filiales françaises d'entreprises américaines qui seraient titulaires de marchés publics pourraient être réquisitionnées par l'autorité américaine pour fournir ces données, ce qui serait contraire au RGPD.

Comme l'a rappelé Mme Laure Bédier, ce n'est pas parce qu'une entreprise est susceptible de commettre une infraction qu'elle a commis cette infraction et qu'on peut la rejeter au stade de la candidature. En revanche, nous avons proposé dans le CCAG de dire très clairement à tout futur titulaire d'un marché public que, quand bien même il serait soumis par un effet d'extraterritorialité des dispositions américaines à des obligations à ce titre, il ne peut

pas enfreindre le RGPD. Nous rappelons dans les CCAG l'obligation de respecter le RGPD, nous précisons en quoi elle consiste. Nous proposons d'y inscrire que toute demande de communication de données de la part d'une administration étrangère devra faire l'objet d'une déclaration à l'acheteur. Nous proposons également d'assortir le non-respect ou la violation de cette obligation de sanctions. L'objectif est de rappeler à toute entreprise qu'elle sera soumise à des sanctions, si elle viole le RGPD, fût-ce en application d'une autre législation.

M. Philippe Latombe, rapporteur. Comment percevez-vous la décision du Conseil d'État concernant le Health Data Hub et les conséquences qu'elle pourrait avoir sur d'autres marchés de ce type ? Cette ordonnance fait suite à la décision de confier à Microsoft l'élaboration d'une plateforme de santé. Après avis de la CNIL, le Conseil d'État a enjoint l'exécutif à rapatrier les données sur un *cloud* souverain à échéance de deux ans. L'ordonnance pourrait avoir des impacts dans d'autres domaines, notamment l'Éducation nationale, qui utilise aussi de nombreux logiciels américains.

M. Benoît Dingremont. Je pense que la décision est assez cohérente avec la logique préconisée dans les CCAG. Autant on ne peut pas sélectionner et rejeter une candidature étrangère, autant on peut insérer dans les clauses du marché des règles de sécurité ou d'implantation de données, si l'implantation sur le territoire européen est la seule façon de garantir la sécurité des données et du système.

Mme Laure Bédier. Je n'ai pas examiné en détail la décision du Conseil d'État, mais un élément important est qu'il s'agit de données de santé, particulièrement sensibles. Dans ce cadre, on peut parfaitement demander le stockage des données sur le territoire national ou européen. Il conviendrait d'examiner si cette décision, concernant des données particulièrement sensibles, pourrait être transposée à d'autres données moins sensibles. Je n'en suis pas certaine.

M. Philippe Latombe, rapporteur. L'accord avec le Health Data Hub prévoyait la localisation des données sur le territoire européen, ainsi que le chiffrement de celles-ci. La clé ne devait appartenir qu'au Health Data Hub et l'opérateur de cloud n'y avait pas accès. Pour autant, le Conseil d'État a estimé qu'il existait un risque de transfert des données à l'étranger et qu'à ce titre, il fallait les transférer dans un *cloud* qui n'était pas soumis au *Cloud Act*. Nous serions heureux que vous nous communiquiez votre analyse de la décision du Conseil d'État. Vous avez par ailleurs évoqué la règle des 50 %. Or, on observe des appréciations différentes de ces 50 % en Europe. Par exemple, les Irlandais sont les principaux hébergeurs des GAFA. Percevez-vous une distorsion de législation ou d'interprétation entre les Irlandais et les Français sur la notion des 50 % ?

Mme Laure Bédier. Je sais que certains pays sont beaucoup plus souples.

M. Philippe Latombe, rapporteur. Ce sont en gros l'Irlande et le Luxembourg.

Mme Laure Bédier. Je ne connais pas leur position exacte concernant le calcul des 50 %.

M. Benoît Dingremont. La règle des 50 % posée à l'article L. 2153-2 du code de la commande publique ne concerne que les marchés de fournitures. Je pense que, s'agissant de l'Irlande, il est surtout fait référence à l'attrait fiscal que ce pays représente pour les services. Les GAFAM profitent de ces dispositions, mais il me semble que la disposition de l'article 85 de la directive ne pourrait s'appliquer pour un marché de services.

M. Philippe Latombe, rapporteur. Cela est vrai pour les services, mais Apple fournit, par exemple.

M. Benoît Dingremont. Le problème est que la directive ne parle pas d'achats de fournitures dans le cadre d'un marché de services. Je suppose que la plupart des dispositifs sur l'implantation des GAFAM en Irlande concerne davantage les services que l'achat par les personnes publiques d'une fourniture.

M. Philippe Latombe, rapporteur. Lors de la précédente audition, un juriste nous a indiqué que l'utilisation des marchés à procédures adaptées (MAPA) n'était pas aussi aisée qu'il semblait.

Mme Laure Bédier. Je vous répondrai en tant que praticienne. Ayant travaillé auparavant à l'Assistance publique-Hôpitaux de Paris (AP-HP), j'ai observé qu'en-dessous des seuils, les acheteurs avaient tendance à appliquer les procédures formalisées afin d'être certains de ne pas être hors du cadre. La problématique est un peu la même que vis-à-vis du délit de favoritisme. Afin d'être certains que les procédures soient adaptées à l'objet du marché, les acheteurs visent le formalisme maximum.

M. Benoît Dingremont. Un enjeu est de professionnaliser les acheteurs pour leur permettre de comprendre qu'ils peuvent utiliser certaines marges de liberté en toute sécurité juridique. La professionnalisation des acheteurs est prévue dans le plan national d'action sur les achats publics durables (PNAPD), que nous co-animons avec le ministère de la Transition écologique. L'objectif est de proposer aux acheteurs de nouveaux outils et méthodes en matière de critères de choix et de clauses d'exécution, notamment afin de renforcer la qualité environnementale de l'offre. Nous espérons, par ce moyen, valoriser des offres européennes et françaises, peut-être plus chères, mais dont la qualité environnementale sera meilleure. Nous espérons que le PNAPD porte ses fruits auprès des acheteurs, mais l'acte d'achat n'est pas une opération simple.

M. Philippe Latombe, rapporteur. Selon les juristes que nous avons entendus, la formation des acheteurs est très pointue, mais essentiellement juridique. La partie « achats » est ainsi perçue comme une zone de risque, qui doit être gérée par la maîtrise du contentieux, un peu au détriment de l'achat lui-même, qui devrait intervenir en premier lieu. Pensez-vous que l'on devrait modifier les formations afin de renforcer le volet « achats » par rapport au volet juridique ? Afin d'inciter les acheteurs à faire du *sourcing*, ils doivent prendre connaissance des besoins, ce qui suppose une connaissance des solutions existantes. Que pensez-vous de la création d'un portail public permettant aux entreprises de communiquer l'état d'avancement de leurs produits ? Devrait-il être hébergé chez vous, éventuellement relayé par des CCI au niveau local ? Ce dispositif pourrait-il permettre à l'ensemble des acteurs d'obtenir une vision complète des solutions ?

Mme Laure Bédier. La conception d'un portail de *sourcing* est une action prévue dans le plan de transformation numérique de la commande publique. L'ensemble des entreprises pourront y présenter leur offre. Par ailleurs, la DAE mène une action spécifique en matière d'innovation.

M. Benoît Dingremont. La DAE travaille à la fois sur la professionnalisation des acheteurs et sur le *sourcing*. Elle a déjà mis en place, il y a quelques années, un portail pour les acheteurs de l'État. Elle participe en outre à l'élaboration du PNAPD qui comporte un volet formation. L'offre de formation juridique à l'achat public est effectivement très importante. Nous tenterons de développer dans le plan les aspects environnementaux et économiques de l'achat public.

Mme Laure Bédier. Je suivi d'accord avec le constat que les acheteurs sont bien formés au droit de la commande publique, mais pas forcément aux aspects opérationnels et à la connaissance de l'offre. Ils sont parfois trop « juristes » et pas assez « acheteurs ».

M. Philippe Latombe, rapporteur. La semaine dernière, nous avons auditionné l'UGAP. Ses représentants ont indiqué qu'ils proposent dans leur catalogue ce qui correspond aux besoins, mais qu'ils ne jouent pas de rôle de conseil. Or, la phase de définition des besoins, en amont des marchés publics, est très importante, car elle permet de simplifier le processus par l'achat de solutions totalement intégrées. L'allotissement n'est pas la solution la plus efficace pour parvenir à cet objectif. Selon un avocat que nous avons auditionné, il devient rapidement ingérable, faute d'une direction des systèmes d'information (DSI) capable de déterminer l'allotissement optimal. Enfin, nous manquons de professionnels de l'informatique dans le secteur public, car ils préfèrent, en général, rejoindre le privé pour une question de rémunération. Il en résulte une simplification dans les besoins, dès le début. Comment pourrait-on traiter cette difficulté ?

Mme Laure Bédier. Comme nous l'avons dit, les personnes formées en droit et non au segment d'achat sont tentées d'adopter les solutions les plus simples « sur étagère », sans vraiment réfléchir à leurs besoins, alors que cette étape est indispensable pour promouvoir la souveraineté. Il est à la fois nécessaire de bien connaître le secteur et d'être capable de définir les besoins avec précision. L'enjeu est d'identifier des acheteurs ayant une bonne connaissance du secteur au-delà des compétences juridiques.

M. Philippe Latombe, rapporteur. La définition des besoins ne se fait pas au niveau des acheteurs.

Mme Laure Bédier. L'acheteur joue néanmoins un rôle de conseil. Il doit pouvoir aider le prescripteur à définir ses besoins avec précision.

M. Benoît Dingremont. Nous pouvons identifier certaines évolutions positives, notamment dans le *sourcing*, qui est proche de la définition des besoins. À partir du moment où l'acheteur d'intéresse au *sourcing*, cela signifie qu'il pense à une nouvelle façon de définir ses besoins au lieu de réitérer le même achat ou d'adopter des solutions intégrées globales. Cinq ans auparavant, lorsque nous parlions de *sourcing* dans une enceinte publique, la réticence était vive et nombre d'acheteurs demandaient s'ils avaient le droit d'y recourir. La situation a beaucoup évolué depuis lors. Aujourd'hui, tous les acheteurs disent pratiquer le *sourcing*, même si cela se fait de façon plus ou moins approfondie. Quoi qu'il en soit, le terme n'est plus tabou et la situation évolue.

M. Philippe Latombe, rapporteur. Y a-t-il d'autres sujets que nous n'avons pas évoqués et que vous souhaiteriez porter à notre connaissance ?

Mme Laure Bédier. Je souhaite simplement redire que nous sommes très encadrés par le droit européen. La formation des acheteurs à l'utilisation des différents outils de la commande publique est une perspective intéressante qui devrait permettre d'orienter l'attention vers les offres européennes.

Audition commune de Mme Servane Augier, directrice générale déléguée de 3DS OUTSCALE, M. Michel Paulin, directeur général d'OVHcloud, et Mme Karine Picard, directrice générale d'Oracle France
(9 février 2021)

Présidence de M. Philippe Latombe, rapporteur.

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

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

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

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

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

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

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

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

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

Nous travaillons, notamment avec M. Michel Paulin, au sein du Comité stratégique de filière, pour pousser ces notions de souveraineté et pour faire en sorte que la filière puisse avancer. Dans le cadre de ce Comité stratégique de filière, nous avons signé un contrat avec les ministères. Nous attendons des engagements forts de l'État sur le fait de réglementer la nécessité d'utiliser un *cloud* de confiance pour les données sensibles pour les administrations et les opérateurs d'importance vitale (OIV). Il est nécessaire d'impulser un mouvement fort pour les administrations et les grandes entreprises d'importance vitale en France. Il y a deux volets. Le premier est le fait de réglementer les choses. La bonne nouvelle est que le Cigref a réalisé une étude récemment. Les membres du Cigref sont prêts à accepter une réglementation supplémentaire parce que les enjeux leur paraissent primordiaux. Le deuxième volet concerne la mise en place d'un label permettant de définir ce qu'est un *cloud* de confiance. Aujourd'hui, le référentiel SecNumCloud porte essentiellement sur les critères techniques. Il en va de même pour le référentiel HDS pour l'hébergement de données de santé. Ces référentiels, labels, ou qualifications n'emportent jamais cette logique que son détenteur

n'est pas soumis à des lois extra-européennes. Cela manque dans le paysage. Il faudra y travailler rapidement. Il faut pouvoir dire : *« Nous, qui répondons aux critères que je vous ai donnés tout à l'heure, nous pouvons l'exposer publiquement, parce qu'une entité publique nous donne le droit de le faire »*. Il sera également très important, dans le cadre de Gaia-X, qui créera des standards à l'échelle européenne, de faire ressortir, au sein des offres qui vont adopter des standards techniques, celles qui sont de confiance au sens où elles garantissent la souveraineté.

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

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

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

Nous sommes aussi certifiés sur les données de santé aujourd'hui. Nous travaillons avec l'ANSSI pour être certifiés SecNumCloud. Nous espérons être un acteur américain qui pourra entrer dans les critères de ce qu'est un *cloud* de confiance. La notion de *Cloud Act* est assez déterminante. Il est important de savoir que le fait qu'un éditeur soit national ne signifie pas qu'il respecte les critères de sécurité. Des investissements doivent être réalisés dans la manière dont sont construits les *clouds*, dans la manière dont on peut contrôler l'ensemble de

la chaîne du cloud (depuis la création de la machine, de la puce, de la base de données, des transferts de la donnée, du *data center*). Ce contrôle de la chaîne complète de la donnée est extrêmement important pour assurer la meilleure sécurité. Devant cette demande de souveraineté de nos clients et en particulier des gouvernements, nous avons travaillé sur de nouvelles offres de *cloud*, que l'on appelle des *clouds* régionaux, qui permettent aux gouvernements ou aux entreprises de disposer, derrière leur pare-feu, de tous les avantages du *cloud* public, en termes de consommation de services, d'innovations, mais aussi de protection des données. Ainsi, pour répondre à votre question, en tant qu'acteur du *cloud* et en tant qu'acteur américain, cela fait plusieurs années que nous travaillons à comprendre les besoins des entreprises privées et publiques en France et en Europe, et de répondre à leurs attentes.

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

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

Quels sont les grands principes d'OVHcloud aujourd'hui ? Le premier est que nous défendons un *cloud* de confiance, par définition technique et par définition légale, dans le sens où techniquement, nous sommes un grand supporter de l'*open source*. Nous travaillons sur des solutions interopérables, ouvertes, réversibles. L'interopérabilité est clé. Pour cela, il faut garantir que les *API* soient documentées, ouvertes, qu'il s'agisse des *API* au-dessus ou en dessous. Il faut faire en sorte que l'ensemble des solutions logicielles soient réversibles. Nous avons aussi une longue tradition d'intégration avec un modèle. Nous construisons nous même nos serveurs. Cela donne une totale traçabilité en France, à partir de composants qui sont achetés à travers le monde. Nous avons aussi la volonté de travailler avec un écosystème. Cet écosystème sera un moyen pour dynamiser la filière européenne et la filière française. Nous investissons massivement. Nous sommes 2 300 aujourd'hui à travers le monde. Nous investissons dans nos 32 *data centers*. Nous venons d'ouvrir un *data center* en Asie, à Singapour, et un autre, à Sydney. Nous investissons dans la Recherche et Développement. Nous avons, comme l'a mentionné Servane Augier, reçu de nombreuses certifications dont tout récemment SecNumCloud, mais également les certifications HDS, Iso 27 001. Nous sommes convaincus qu'OVHcloud a les moyens de proposer des solutions alternatives autour du *cloud* de confiance.

Qu'est que la souveraineté ? Pour nous, la souveraineté n'est pas le nationalisme, le patriotisme, le protectionnisme, mais la capacité pour des États, pour des entreprises, pour des individus, de pouvoir choisir. À la fois en termes légaux, techniques, et de pratiques

concurrentielles, certains acteurs ont tendance à créer des monopoles fermés, qui bloquent les clients dans des systèmes. C'est l'inverse de ce que nous pensons être la souveraineté.

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

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

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

Il convient d'être extrêmement précis sur quatre éléments :

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

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

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

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

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

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

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

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

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

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

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

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

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

Cependant, ce choix n'est pas toujours réalisé après avoir effectué un réel examen de ce qui est accessible sur le marché. Des décisions sont prises de manière un peu hâtive, alors qu'il existe des solutions, quasiment aussi rapides, avec des acteurs français. Pendant la crise du Covid, nous avions un programme de solidarité *Act For Life*. Un de nos partenaires a monté en deux jours le site de la réserve civique sur notre *cloud*. De nombreux sites se sont

montés très vite sur des *clouds* souverains pendant la période. Pourquoi n'a-t-il pas été possible de monter celui du prêt garanti aux entreprises (PGE) sur un *cloud* français ? Je ne sais pas le dire. Sur le dossier du Health data Hub (HDH), qui est beaucoup plus complexe en termes de services utilisés, le critère de rapidité de mise en œuvre a prévalu. En revanche, sur un site internet, je m'interroge un peu.

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

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

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

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

M. Michel Paulin. Je ne suis pas tout à fait d'accord. À ma connaissance, avec OUTSCALE, nous sommes largement moins chers que tous les *hyperscalers*. Vous pouvez regarder tous les *benchmarks* publics : nous sommes beaucoup moins chers. La notion de compétitivité en termes des prix/performance n'est pas un argument opposable aujourd'hui. C'est plutôt l'inverse. Le Cigref se plaint de la position dominante de certains des acteurs qui profitent de leur position dominante pour imposer leur *cloud*. Les acteurs de SaaS en particulier imposent le stade en dessous pour pouvoir justifier de l'évolution technologique et

l'augmentation des prix. Aujourd'hui, un certain nombre de clients se retrouvent, avec des *hyperscalers*, dans des situations où leurs coûts augmentent fortement. De plus, ces *clouds* sont fermés, sans *API* et ne sont ni transparents ni réversibles. Nous sommes dans une double problématique. De notre côté, nous travaillons pour fournir des solutions souveraines, avec des *API* ouvertes, de l'*open source*, avec des prix largement plus compétitifs que la majorité des *hyperscalers*. Nous nous sommes toujours engagés dans la filière à maintenir nos prix à un niveau compétitif, quelles que soient les contraintes posées par l'État.

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

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

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

Le fait de dire que les acteurs ne sont pas capables de répondre à l'ensemble des demandes est une facilité intellectuelle. Bien souvent d'ailleurs, il n'y a pas d'appel d'offres. L'effort d'analyse n'a pas été fait. Aujourd'hui, sur un sujet comme le web, sur lequel nous sommes numéro 1 français, nous avons des choses à faire valoir. Nous ne sommes pas numéro 1 par hasard. Nous sommes un des hébergeurs les plus puissants sur les grands et les petits sites. Sur ce sujet, nos arguments sont nombreux et prouvent que nous possédons les

solutions. Faut-il encore être consultés et pouvoir répondre de manière équitable et sans exclusivité. Il faut qu'il y ait de la concurrence, de l'innovation. C'est important. Vous connaissez nos positions publiques sur un certain nombre de sujets : nous attendons l'appel d'offres et nous y répondrons.

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

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

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

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

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

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

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

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

a été remonté il y a quinze jours. Cette pratique commerciale des *vouchers* biaise la concurrence. Souhaitez-vous que le législateur, français ou européen, légifère sur ce sujet ?

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

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

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

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

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

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

puissants, avec des acteurs qui sont aidés. Dans certains domaines, l'informatique ou le digital, il n'y a plus qu'un ou deux acteurs au niveau mondial. Prenez le *search* ou les grands domaines digitaux autour des réseaux sociaux.

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

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

Mme Karine Picard. Nous militons pour les mêmes choses. Nous militons pour la transparence depuis toujours. Pour cette raison, nous n'émergeons nos solutions que sur des *clouds* sur lesquels nous pouvons garantir l'intégralité, la sécurité, la localisation des données et qui les opère. Je suis d'accord avec vous. Nous nous battons contre d'autres vendeurs qui hébergent chez Google, Amazon, et autres, sans avoir la garantie de la chaîne complète de la sécurité de la donnée. Leurs clients ne peuvent pas choisir avec qui ils veulent travailler. L'ouverture, la transparence, la réversibilité sont des sujets sur lesquels nous travaillons, depuis toujours, en tant qu'opérateur de cloud. C'est de cette façon que nous nous sommes différenciés d'Amazon, Google, etc. De plus, nous travaillons depuis toujours sur du *BtoB*. Les données de nos clients n'appartiennent qu'à nos clients. En aucun cas, nous ne ferons du *business* sur la donnée. Il y a une différence entre les *providers* de *cloud* qui font du *BtoC* et ceux qui font du *BtoB*. C'est aussi un élément de pédagogie envers les citoyens, qui ne comprennent pas forcément toutes ces subtilités.

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

Mme Servane Augier. Dans les discussions à la direction générale des entreprises (DGE), avec le Comité stratégique de filière, nous avons travaillé sur l'éventuel renforcement de la loi de blocage qui viendrait en contrepoids du *Cloud Act*, et qui viendrait flécher la donnée sensible vers des *clouds* de confiance. Nous appelons à la création d'un label permettant de clarifier le paysage et d'adresser des messages clairs aux futurs clients. La souveraineté est la capacité à choisir. Cependant, pour choisir de manière éclairée, il est utile d'avoir des panneaux explicatifs. Les acteurs ne peuvent pas dresser eux-mêmes les panneaux, au risque d'être juges et parties. Ce que nous décrétons est moins fort que ce que quelqu'un

peut nous attribuer comme mérite. C'est pourquoi nous sommes très enclins à passer des certifications. Nous pensons que la confiance se prouve. Je souhaite que l'État mette en place un système permettant de savoir quels labels garantissent le respect des critères de non-soumission à des réglementations extra-européennes.

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

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

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

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

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

M. Michel Paulin. Je me permets de « challenger » cette affirmation. L'une des implications de *Schrems* II est que le fournisseur de *cloud* est exclusivement soumis à la juridiction de l'Union européenne, à l'article 48 du RGPD. Or le *Cloud Act*, dans la juridiction, impose aux acteurs américains de fournir des données sur injonction. C'est cadré, mais selon

moi, il existe un enjeu. Dès qu'un acteur est soumis au *Cloud Act*, il est exposé à ne pas être conforme à *Schrems* II.

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

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

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

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

Mme Servane Augier. Je vois se multiplier les webinaires à destination des clients pour leur parler des conséquences de *Schrems* II, de ces clauses contractuelles. Il existe une difficulté de compréhension. La première intervention serait de créer un *vademecum* à l'intention des entreprises françaises sur ce qui fonctionne, sur les aspects où la prudence est de mise, sur les contrats à revisiter. Aujourd'hui, tout le monde improvise. En fonction de la sagacité des *data protection officers* dans les entreprises, certains sujets seront soulevés ou non. Un petit guide à l'attention des entreprises sur les points de vigilance serait pertinent. Nous entendons parler d'amendes qui peuvent être considérables. Il ne faut pas punir l'économie française avec ces difficultés contractuelles.

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

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

Mme Karine Picard. Il est nécessaire de clarifier *Schrems* II, car les éditeurs ou les entreprises n'en comprennent pas les conséquences. Nous sommes conformes au RGPD, qui est clair, mais il faudra apporter de la clarté juridique sur *Schrems* II pour que nous puissions nous positionner. Le flou pour les entreprises, en période de Covid, n'est pas opportun. Elles doivent investir dix fois plus rapidement pour s'adapter et faire face à la crise. Le flou autour des contrats qu'elles auront le droit de conclure et des risques qui existent

retardera les entreprises dans leur choix et donc dans leur transformation digitale, ce qui n'est dans l'intérêt de personne. Cette clarté est extrêmement importante. Il faut laisser la possibilité aux entreprises de choisir les solutions les plus sûres et les plus pertinentes par rapport à leur métier et à leurs besoins. La clarté est indispensable, étant donné la situation actuelle. Les entreprises n'ont pas arrêté leurs investissements digitaux. Il convient de les accompagner au mieux dans la clarté.

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

Mme Servane Augier. Il serait important que la doctrine de l'État soit plus claire et qu'elle soit descendue dans les administrations déconcentrées et dans les collectivités territoriales. L'UGAP a fait un travail formidable pour mettre en place un marché de référencement qui apporte des outils. Parmi ces derniers, tous les *cloud providers* sont référencés, les *cloud providers* français, les *cloud providers* américains. Il n'existe pas de mode d'emploi pour l'accompagner, de doctrine de l'État disant : *« nous vous donnons des outils, parce que vous avez besoin de choix, d'agilité dans votre transformation* cloud *en région. Nous vous recommandons de faire tel ou tel choix en fonction de tel ou tel critère »*. Il faut clarifier, prendre parti et dire : *« Nous, en tant qu'État, recommandons que les données de santé locales, que les données financières, que les données des citoyens restent sur des* clouds *de confiance. Cela signifie de faire appel à tel ou tel fournisseur pour tel usage. Vous pouvez choisir plus largement pour telle autre typologie d'usage. »*

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

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

pouvons pas le remporter en raison de notre nationalité. Les vendeurs ont besoin de clarté pour savoir quels types d'appels d'offres sont ouverts ou non.

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

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

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

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

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

M. Philippe Latombe, rapporteur. Nous avons décidé d'ouvrir une séquence sur la formation fin mars/début avril. Le sujet de la formation primaire jusqu'aux grandes écoles sera abordé. Nous sommes preneurs de vos propositions sur les différentes thématiques que

nous évoquerons au sein de la mission. N'hésitez pas à continuer à contribuer par des écrits que nous annexerons au rapport.

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

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

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

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

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

Audition commune, ouverte à la presse, de M. Jean-Noël de Galzain, président d'HEXATRUST, M. Stéphane Volant, président du Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE), et de Mme Florence G'Sell, professeure de droit à l'université de Lorraine, membre du Club des juristes
(11 février 2021)

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

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

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

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

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

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

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

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

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

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

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

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

M. Philippe Latombe, rapporteur. Vous oubliez Pékin.

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

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

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

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

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

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

On nous parle d'un grand plan quantique national. En tant qu'utilisateur, je me réjouissais de ce plan, car je pensais que nous étions précurseurs sur le quantique, qui ne fait pas beaucoup parler de lui. En m'intéressant ce matin aux statistiques, j'ai découvert que la Chine avait déposé l'année dernière 1 157 brevets en matière de quantique, que les USA en

avaient déposé 363, la Grande-Bretagne 29, l'Allemagne 23 et la France 9. C'est dire notre retard, y compris sur ce sujet.

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

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

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

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

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

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

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

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

Tout d'abord, il faut définitivement soutenir la R&D, non seulement celle des grands, mais aussi celle des PME et celle des start-up. Il nous faut également écouter les utilisateurs, qui ne veulent pas qu'on les contraigne à prendre des solutions souveraines exorbitantes et

malcommodes, au motif qu'elles sont souveraines. Le coût de la souveraineté représente un supplément de 10 % à 15 %. C'est une assurance, mais nous ne pourrons pas aller au-delà. Encore faut-il que nous nous saisissions de la question des critères de la souveraineté et que les entreprises soient assurées, pour 15 % de plus, de ne pas se faire piller leurs données et de pouvoir parler à leurs clients en toute tranquillité.

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

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

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

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

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

En matière de numérique, nous sommes aujourd'hui ballottés entre deux mondes, pour reprendre la formule d'Eric Schmidt, le patron de Google à l'époque. Nous sommes ballottés entre un monde numérique chinois organisé au bénéfice des organisations gouvernementales et du système chinois, et le reste du monde emmené par les Américains. Une opportunité historique se présente à nous, celle de créer le numérique de confiance, c'est-à-dire un environnement numérique éthique, protecteur des données personnelles, et garantissant les critères de liberté, d'autonomie et donc de souveraineté.

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

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

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

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

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

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

Dans notre manifeste, nous avons énoncé cinq grandes mesures.

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

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

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

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

La quatrième mesure est de financer les ETI, les PME et les start-up de croissance. Cet aspect est essentiel. Arrêtons de croire que nous allons changer le monde en investissant de l'argent dans les grandes entreprises. Si nous réservons de l'argent aux PME, start-up et ETI, et si leurs propositions de valeur séduit les utilisateurs, alors nous parviendrons à attirer les grands intégrateurs, les grands financeurs et les grandes banques. Le cercle vertueux fonctionnera, puisque nous créerons de nouveaux besoins et de nouveaux marchés. À cette création de valeur, succède un ruissellement. Nous avons pris ce ruissellement à l'envers. Il doit commencer par les petits, qui seront ensuite aidés par les grands pour passer à l'échelle supérieure. Le fait de financer les PME et les ETI implique de mettre des moyens à la Banque européenne d'investissement, afin que nous y ayons accès.

S'agissant d'une PME comme Wallix, la société que je dirige, la Banque européenne d'investissement propose de l'aide, ce qui est un point positif. Mais quand nous demandons cette aide, nous nous trouvons avec des taux de prêts allant de 13 % à 17 % par an. C'est prohibitif. Ainsi, les solutions de financement existent, mais elles sont inaccessibles aux PME et aux ETI. Il faut par conséquent changer les mentalités. Aujourd'hui, une entreprise comme Thales peut emprunter à 1 % ou à 3 %. Nous devons être en mesure de le faire également. Il

faut de grands fonds d'investissement permettant aux investisseurs qui sortent au fur et à mesure de nos entreprises de ne pas avoir à revendre systématiquement l'entreprise à un fonds américain ou à un grand industriel américain, qui pourra, quant à lui, payer la juste valeur pour les entrepreneurs.

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

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

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

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

Cette affaire exprime bien la manière dont nous pouvons envisager la question de la souveraineté numérique, à travers l'idée d'un bras de fer entre les États et les plateformes. Même si des règles juridiques s'appliquent au monde virtuel et aux plateformes, celles-ci ont acquis une telle force de frappe et une telle indépendance qu'elles sont en mesure de faire ce qu'elles veulent, de fonctionner en se référant d'abord à leurs conditions d'utilisation. Ces plateformes s'appuient aussi sur le fait qu'elles sont implantées aux États-Unis et qu'elles se conforment avant tout à la législation américaine.

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

Le volet de la souveraineté comprend bien évidemment d'autres aspects. Qui dit souveraineté dit aussi indépendance, c'est-à-dire indépendance technologique. Nous avons pris conscience, à la faveur de la crise sanitaire, de notre dépendance à des technologies principalement américaines – nous sommes aujourd'hui sur Zoom et j'enseigne avec ces outils

depuis presque un an maintenant. De fait, nous avons en permanence le sentiment de buter sur cette dépendance technologique pour un grand nombre de sujets, en particulier la question du stockage des données.

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

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

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

M. Stéphane Volant. J'ai été confronté, et les adhérents du CDSE le sont encore, à ce genre de difficulté dans des appels d'offres. La vraie difficulté n'est pas de savoir si ceux qui décident de recourir à des solutions non souveraines sont des naïfs. Avant cela, il faut se préoccuper des critères que la loi impose dans les appels d'offres. Quand vous êtes face à diverses solutions dont aucune ne vous est officiellement interdite, que vous trouvez une solution moins coûteuse et beaucoup plus performante que les autres, et que la plus coûteuse porte un drapeau national, vous n'allez pas pour autant retenir la solution souveraine. Tout d'abord, ce n'est pas votre intérêt. Ensuite, parce que certains règlements d'appel d'offres vous encouragent à vous tourner vers le moins-disant et non vers le mieux-disant.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

M. Philippe Latombe, rapporteur. Pour élargir le sujet du *cloud*, vous dites qu'il faudrait nous doter d'un *Buy European Act*, en parallèle du *Small Business Act* américain. Qu'est-ce qui permettrait aujourd'hui de le mettre en place ? Doit-on le faire au niveau

européen, ou bien au niveau national, si l'Europe n'y parvient pas dans un premier temps ? Comment pouvons-nous nous affranchir d'un certain nombre de règles européennes, notamment sur les marchés publics, si nous n'atteignons pas cet objectif global ? Vu le nombre de pays européens et le processus de décision européen, comment procéder ?

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

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

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

Je suis comme nous tous extrêmement soucieux de l'intérêt national et parfaitement conscient des atteintes à notre souveraineté, inhérentes à l'utilisation de ces solutions étrangères. Mais attention à ne pas nous bercer d'illusions. Si le client ne retient pas de solution souveraine et nationale à 85 %, y compris quand il est public ou de défense, ce n'est pas parce qu'il est idiot ou antipatriotique, mais probablement parce qu'il n'y a pas sur étagère de solution concurrentielle dans ce domaine.

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

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

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

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

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

Il s'agit donc assurément d'entreprises qui, pour le coup, n'auront plus aucun contrôle sur leur souveraineté IT.

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

De plus, afin de donner l'exemple, je crois que nous ne devons pas hésiter à commencer au niveau national, comme nous l'avons fait pour la taxe GAFAM. Cet effort de reconstruction doit être initié dès à présent : en effet, au sortir de la crise consécutive à la crise sanitaire, des milliers de milliards d'euros seront investis dans de nouvelles infrastructures, dans la modernisation et dans la transformation digitale, de la sphère privée comme de la sphère publique. Ces investissements concerneront tout le monde, c'est pourquoi il faut, selon moi, réserver une part de l'investissement public à l'émergence d'une industrie européenne, qui crée de l'emploi local, favorise la création de centres de données locaux et nous permet de reprendre la main sur notre destin, en lieu et place du sempiternel argument juridique utilisé pour tenter de surnager dans un monde numérique que nous ne contrôlons pas. Si nous n'avons pas les clefs du numérique, nous continuerons à courir après le numérique de quelqu'un d'autre, qui, au bout d'un moment, utilisera l'intelligence artificielle en tant que service après-vente pour les questions juridiques, tout en continuant à investir dans son avance technologique, face à laquelle nous avons pourtant les moyens d'exister. Dans le domaine de la santé, comme dans les télécoms, l'IT, le numérique ou encore la cybersécurité, nos chercheurs, nos start-up et nos entrepreneurs travaillent pour des entreprises américaines, notamment. Nous disposons donc de tout le potentiel nécessaire.

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

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

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

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

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

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

Pour ma part, j'apprécie les travaux du HDH qui mène de grands projets étendards : nous avons ainsi proposé, dans le cadre du comité stratégique de filière, de mettre à niveau la cybersécurité de tous les établissements hospitaliers de France (CH et CHU), parce qu'il s'agit de projets dans lesquels toute l'industrie entend intervenir, au côté de l'État, pour faire exister les solutions et infrastructures et les mettre en pratique dans le cadre de projets qui feront progresser notre industrie sur un sujet concret. Je ne connais pas tous les détails à propos du HDH et n'entends pas trop m'étendre sur ce sujet qui s'est avéré extrêmement sensible, mais je peux témoigner du fait que le HDH a fait le choix de mêler l'utilisation d'un *cloud* Azure qui, visiblement, représentait la solution à ses besoins du moment, à des outils de cybersécurité qui permettent de contrôler les accès, d'identifier les utilisateurs qui accèdent à tel ou tel type de données et de tracer l'activité autour des accès internes à ce *cloud*. Un tel montage ne nous prémunit pas des problématiques juridiques, mais d'un point de vue technologique, il offre tout de même de la visibilité sur les accès aux données stockées dans ce *cloud*. Or, lorsque nous commencerons à sauvegarder des données publiques dans ce *cloud*, nous devrons *a minima* être capables de savoir exactement qui fait quoi et à quel moment, de manière à pouvoir mettre un point d'arrêt aux éventuels accès illégaux ou non appropriés.

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

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

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

En effet, je ne vois pas bien comment nous pourrions initier un tel bras de fer, même si nous nous contentons par exemple de dire que nous ne voulons pas, en France, dans nos

appels d'offres, d'entreprises ou de filiales d'entreprises américaines. Cela créerait des difficultés à l'échelle intracommunautaire.

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

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

M. Jean-Noël de Galzain. L'Angleterre constitue le plus gros marché d'Europe en matière d'IT : elle représente en effet 15 % à 17 % du marché européen. Il s'agit toutefois d'un marché très libéral, qui a toujours été utilisé par les fournisseurs américains de solutions pour s'installer en Europe. Cela ne changera pas, c'est pourquoi la sortie de l'Angleterre ne modifiera pas fondamentalement le *business* des acteurs d'HEXATRUST.

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

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

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

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

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

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

M. Stéphane Volant. Quels seraient les critères de souveraineté qu'il faudrait mettre en exergue pour prétendre être souverain et faire de cette souveraineté une valeur ajoutée, de telle sorte que, sans passer par la contrainte, les solutions définies et validées comme souveraines, en France, par un organisme indépendant, puissent être retenues, parce qu'elles

sont concurrentielles, sur la base de fonctionnalités identiques, souveraines et protectrices, quitte à ce que leurs prix soient légèrement supérieurs ? Bref, pouvez-vous nous éclairer, en droit, sur les conditions de la souveraineté ?

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

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

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

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

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

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

Je souhaite toutefois mettre un bémol sur ces inquiétudes : dans le *Cloud Act*, nous partons de l'hypothèse qu'une entreprise américaine, qui a le contrôle de données pourtant

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

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

Je n'ai pas sous les yeux toutes les données chiffrées relatives à ces demandes de communication. Selon des rumeurs, elles auraient explosé auprès d'Amazon ou de Microsoft, mais je ne dispose pas de chiffres précis. Néanmoins, à l'évidence, pour résoudre ce problème, il est certain qu'il convient d'en passer par un *cloud* souverain : j'ai par exemple eu l'occasion d'échanger avec la DGFiP qui dispose actuellement de systèmes de stockage très élaborés. Rien ne nous empêche donc d'avancer maintenant que GAIA-X est en place.

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

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

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

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

La question des acquisitions est également évoquée dans le *Digital Market Act*. Or, dans le secteur du numérique, le scénario des *killer acquisitions* s'avère parfaitement connu : de jeunes pousses innovantes, disruptives et prometteuses, qui fonctionnent bien et font parler

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

Enfin, je souhaite évoquer la question de la coopération à l'échelle européenne. En effet, parce qu'il s'adresse aux très grandes plateformes, le *Digital Market Act* désigne la Commission en tant qu'autorité de contrôle, tandis que, dans le *Digital Services Act*, comme dans d'autres textes européens, les autorités nationales, réunies au sein d'un comité européen sur les services numériques, conservent la main. Ce comité de coordination répond bien entendu à d'importants enjeux politiques, mais comment l'articuler avec les autres autorités pour aboutir à un dispositif qui fonctionne mieux et plus vite ? Est-il complètement exclu de constituer une autorité de contrôle numérique à l'échelle européenne ? J'ai en effet le sentiment qu'en matière numérique, il convient de raisonner d'abord à l'échelle européenne.

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

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

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

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

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

En revanche, il me paraît urgent de considérer le fait qu'un certain nombre d'entrepreneurs ne sont pas attirés par l'idée de devenir milliardaires à tout prix. D'aucuns associent le profil du patron à la volonté de « s'en mettre plein les poches », mais il faut avoir à l'esprit qu'un certain nombre d'entrepreneurs sont séduits par l'idée de créer des géants mondiaux comme Schneider Electric, Alstom et d'autres sociétés françaises qui ont fantastiquement bien réussi. Or, pour y parvenir, ils ont besoin d'un certain nombre d'instruments qui fonctionnent, à savoir des solutions de sortie pour les investisseurs, c'est-à-dire des solutions permettant de réaliser, sans avoir à revendre là où les capitaux sont les plus nombreux, là où ils s'achètent le plus cher.

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

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

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

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

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

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

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

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

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

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

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

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

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

M. Philippe Latombe, rapporteur. Je vois bien que les entrepreneurs font tout leur possible pour aider l'ensemble des citoyens à surmonter la crise. Notamment dans le domaine

du numérique, nombre d'initiatives ont vu le jour, au titre desquelles nous devrons remercier l'ensemble des écosystèmes. Si notre mission peut, à sa mesure, vous aider, elle le fera avec le plus grand des plaisirs.

Audition, ouverte à la presse, de Mme Stéphanie Combes, directrice du groupement d'intérêt public Plateforme nationale d'accès aux données de santé (Health Data Hub)
(18 février 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. L'audition de ce jour s'inscrit dans notre cycle consacré à la souveraineté numérique et au numérique en santé. La structure Health Data Hub vise à faciliter l'accès à l'ensemble des données de santé, afin de promouvoir la recherche et l'innovation dans ce domaine. Son régime juridique s'appuie sur une base législative : il est défini à l'article 41 de la loi du 24 juillet 2019 portant sur l'organisation et la transformation du système de santé. La création officielle du Health Data Hub est intervenue le 30 novembre 2019. Elle s'inscrit dans le cadre du plan sur l'intelligence artificielle que le Président de la République a lancé en 2018 ainsi que dans une stratégie globale de numérisation accélérée de notre système de santé.

Ce dossier est un concentré des sujets qui intéressent notre mission d'information. Il interroge notre capacité à procéder à des choix opérationnels qui garantissent à la fois la protection des données de nos concitoyens et un niveau le plus élevé possible de performance. Il s'agit de numériser rapidement notre système de santé pour gagner en maturité sur certaines technologies clés pour l'avenir de la protection en santé de nos concitoyens et de rendre un service d'une qualité toujours croissante. Nous avons également – et l'actualité de ces derniers jours nous le rappelle à nouveau – le devoir d'assurer la plus haute sécurité possible de nos systèmes d'information contre les cyberattaques. Nous nous réjouissons donc, Mme Stéphanie Combes, de pouvoir échanger avec vous sur ces différents sujets.

M. Philippe Latombe, rapporteur. Je vous remercie d'avoir accepté d'échanger avec nous. Je souhaite vous interroger sur trois points en particulier.

J'aimerais d'abord que vous nous présentiez le Health Data Hub : son organisation, son fonctionnement, les principaux choix techniques opérés et son actualité pour l'année 2021. Il me semble important de donner le maximum de publicité à cette plateforme qui constitue un outil de pointe pour soutenir la recherche et l'innovation en santé.

Je souhaiterais également savoir comment l'action du Health Data Hub s'articule avec les autres hubs de données de santé en cours de constitution – le Ouest Data Hub par exemple, dont nous auditionnerons les représentants plus tard ce jour. Il s'agit pour nous de comprendre comment le Health Data Hub s'intègre dans l'écosystème du numérique en santé.

Le second sujet que je souhaite aborder avec vous a trait au cœur des travaux de notre mission d'information : la souveraineté numérique dans le domaine de la santé. Comment percevez-vous cet enjeu et comment l'avez-vous intégré à vos choix opérationnels ? La décision de recourir à Microsoft pour héberger les données de santé recueillies par le Health Data Hub a fait l'objet de critiques et d'un recours devant le Conseil d'État. Le ministre des solidarités et de la santé, M. Olivier Véran, s'est finalement engagé à ce que le transfert du Health Data Hub vers un autre hébergeur que Microsoft intervienne dans un délai compris entre douze et dix-huit mois. Je souhaiterais donc bénéficier d'un point d'étape de votre part à ce sujet. Cela constituera également l'occasion d'échanger sur l'initiative européenne GAIA-X.

Enfin, et M. le président l'a souligné, l'actualité récente est marquée par des cyberattaques contre les systèmes d'information des établissements de santé. Face à la sophistication de la menace cyber, comment est-il possible, selon vous, de garantir un niveau de protection maximale à nos infrastructures numériques, en particulier dans le domaine de la santé ?

Mme Stéphanie Combes, directrice du groupement d'intérêt public Plateforme nationale d'accès aux données de santé (Health Data Hub). Le projet du Health Data Hub a trouvé ses racines dans les travaux sur l'intelligence artificielle rendus par M. Cédric Villani en 2018. Il y faisait la promotion des plateformes de partage de données dans différents secteurs – la santé constituant un secteur prioritaire à ce sujet. Une mission de préfiguration et d'expertise a alors été commandée par la ministre de la santé de l'époque, Mme Agnès Buzyn. J'étais rapporteur de cette mission de préfiguration, dont le rapport a été rendu à la fin de l'année 2018. L'année 2019 a été consacrée à la préfiguration de cette structure, par des travaux législatifs et d'infrastructures technologiques. La structure a été créée à la fin de l'année 2019 et fonctionne maintenant depuis un peu plus d'un an.

Ce projet s'inscrit dans une démarche large portée par le ministère de la santé. La feuille de route du numérique en santé est particulièrement ambitieuse. Le Health Data Hub est l'une des trois plateformes numériques qui doivent être bien articulées : une plateforme pour les citoyens, proposant des applications pour les aider dans leurs soins ; une plateforme pour les professionnels de santé, prévoyant des outils pour les accompagner dans leurs activités ; et, enfin, le Health Data Hub qui s'apparente à une plateforme de recherche et développement.

La structure Health Data Hub regroupe 56 parties prenantes, réparties en neuf collèges – ce hub doit représenter l'ensemble de l'écosystème des données de santé, qui est extrêmement vaste. L'État, bien sûr, y est présent : onze directions de l'État sont parties prenantes ; parmi elles, une direction du ministère de la santé et une direction du ministère de la recherche siègent au conseil d'administration. La Caisse nationale de l'assurance maladie (CNAM) est également un partenaire clé du projet. Les autres collèges sont formés par les organismes d'assurance maladie complémentaire ; les établissements de recherche et d'enseignement ; les établissements de santé ; les représentants des professionnels de santé et des usagers ; les agences, opérateurs et autorités publiques indépendantes ; et, enfin, les industriels. L'assemblée générale réunit l'ensemble de ces parties prenantes ; le conseil d'administration, quant à lui, réunit un représentant de chacun des collèges, à l'exception de l'État qui en a deux. Le financement du Health Data Hub est majoritairement public : la structure bénéficie de vingt millions d'euros par an, dont une moitié provient de l'objectif national de dépenses d'assurance maladie (ONDAM) et l'autre moitié du fonds de transformation de l'action publique, un outil de financement de l'innovation.

Le Health Data Hub doit fournir un accès simplifié aux données de santé en France pour améliorer la qualité des soins et l'accompagnement des patients. La plateforme s'adresse aux acteurs qui animent des projets de recherche et poursuivent une finalité d'intérêt public ; ceux-ci doivent soumettre un dossier pour accéder aux données de santé. La mission du Health Data Hub s'articule autour de quatre missions principales. Tout d'abord, la plateforme est un guichet unique. L'institut national des données de santé (INDS), créé par la loi de 2016, jouait déjà ce rôle : un porteur de projet devait monter un dossier de demande pour accéder aux données de santé ; celui-ci était soumis à la Commission nationale de l'informatique et des libertés (CNIL), seule autorité compétente pour autoriser un traitement de données ; enfin, le porteur de projet déposait son dossier à l'INDS.

Nous avons cherché à élargir les missions de ce guichet. En effet, une fois que la CNIL avait autorisé le traitement de données, le porteur de projet pouvait rencontrer des difficultés d'accès aux données car celles-ci pouvaient être éparpillées ou bien impossibles à traiter en raison de problèmes technologiques. Par le Health Data Hub, nous souhaitons apporter un service jusqu'à la réalisation de l'étude. La plateforme sécurisée donne accès à un espace projet, où nous versons les données autorisées dans le cadre des projets et les utilisateurs pourront les traiter avec des logiciels de programmation à l'état de l'art. L'utilisateur n'a accès ni aux données des autres utilisateurs, ni à davantage de données que nécessaire pour son projet. De la même manière, il ne peut pas sortir les données de l'espace projet et toutes ses activités sont tracées. Mais cela n'est pas une obligation : le Health Data Hub n'est pas une plateforme unique. Si certains acteurs disposent déjà de plateformes technologiques au bon niveau de sécurité, alors il n'est pas besoin de passer par le Health Data Hub. Cependant, la mission de préfiguration a montré que beaucoup d'acteurs ne disposent pas de telles plateformes et il est très coûteux de mettre sur pied une infrastructure dotée des bons niveaux de sécurité et des fonctionnalités adéquates.

La plateforme technologique met à la disposition de ses utilisateurs un catalogue de données. La loi a élargi le système national des données de santé (SNDS) à l'ensemble des données associées à un remboursement de l'assurance maladie. Il est évident que toutes ces données ne seront pas versées à la plateforme technologique du hub – cela n'est ni viable ni souhaitable techniquement, financièrement et scientifiquement. Nous nous posons plutôt la question suivante : quelles données du patrimoine de données de santé français sont intéressantes pour la communauté scientifique et de l'innovation ? Un comité stratégique, piloté par l'État, élaborera une priorisation de ces données. Suite à cette priorisation, une liste des bases du catalogue sera établie : elle sera prise par arrêté après avis de la CNIL et sera mise à jour régulièrement.

La dernière mission du Health Data Hub est une mission d'animation. Beaucoup d'initiatives existent sur le territoire et il est important de les agréger afin de générer un impact à l'échelle européenne et internationale. Il faut, pour y arriver, connecter entre elles les initiatives existant dans les différents établissements de santé – cela permettra d'atteindre une masse critique. Le Health Data Hub poursuit cet objectif.

Le SNDS, créé en 2016, est la base des feuilles de soin pseudonymisées pour servir à des fins de recherche. Il constitue une base unique en son genre au niveau international, car la centralisation du système de santé français permet d'obtenir la consommation de soins de l'ensemble de la population. Cela est extrêmement intéressant pour la recherche. Néanmoins, il s'agit d'une base médico-administrative : elle ne comprend, par exemple, ni résultats d'analyses, ni scanners. Il est donc intéressant d'associer cette base avec d'autres.

C'est ce qu'a fait la loi sur l'organisation et la transformation du système de santé en 2019 : cette loi a créé le hub et a élargi le SNDS. Le SNDS constitue un système de base, qui regroupe des données de registre, des cohortes de recherche, des entrepôts de données hospitalières et la base de l'Assurance maladie. Le catalogue du hub présentera une sous-catégorie, constituée par les données du SNDS, dont les bases seront chaînées avec celles de l'Assurance maladie pour élargir la capacité à les réutiliser. Cela est fait en partenariat avec les gestionnaires de bases de données : une convention est signée qui fixe les modalités et les règles de partage. Ainsi, nous discutons aujourd'hui avec un grand nombre d'acteurs pour concevoir ce catalogue – il ne s'agit pas du tout d'un mécanisme d'aspiration des données, comme cela a pu être dit.

Une première version du catalogue a pris forme dans l'entrepôt COVID, autorisé par l'arrêté du 21 avril 2020. Il rend disponible la base du SNDS *fast-track* avec les données de

l'Assurance maladie issues du programme de médicalisation des systèmes d'information (PMSI) et les données de Santé publique France. Les données du système de vaccins y seront également bientôt disponibles.

Que nous manque-t-il pour mettre en œuvre ce catalogue, qui constitue l'ambition clé du Health Data Hub ? Un décret est toujours manquant – sa publication est attendue au mois de février ou de mars 2021. Le comité stratégique doit également se réunir, afin de définir la liste des bases du catalogue, qui sera prise par arrêté après avis de la CNIL. Il est essentiel de pouvoir poser tous ces jalons avant le milieu de l'année 2021. Le Health Data Hub a été lancé en 2019 ; nous ne pouvons pas nous permettre d'accumuler du retard dans la mise en place du catalogue.

L'accès aux données du catalogue ne se fait pas du tout en *open data* – les règles habituelles s'y appliquent. En revanche, le caractère centralisé des données facilite les temps d'accès, l'accès à des logiciels métier adaptés – notamment en cas d'usage pour l'intelligence artificielle – et les chaînages. Ainsi, le Health Data Hub ne va pas remplacer les autres initiatives, notamment les plateformes locales déjà existantes. Par exemple, l'entrepôt de l'Assistance publique-Hôpitaux de Paris (AP-HP) n'a pas besoin du Health Data Hub pour conduire la plupart de ses projets. Mais le Health Data Hub pourrait l'intéresser pour certains d'entre eux – ainsi, nous travaillons actuellement avec l'AP-HP sur une dizaine de projets, ce qui prouve bien nos intérêts communs et complémentaires.

Le Health Data Hub permettra en premier lieu le croisement des sources. Un projet s'appuyant sur les données d'un établissement de santé est intéressant, mais il lui manque les données de santé de ville et peut-être les données des autres établissements de santé. Le chaînage entre les données de l'Assurance maladie et celles de l'établissement de santé permettra d'adopter une approche en parcours de soins et de conduire des projets qu'il n'est pas possible de concevoir autrement. Aujourd'hui, un chaînage, c'est-à-dire un croisement de sources de données, peut durer trois à quatre ans en France. L'ambition du Health Data Hub est de réduire ce délai à six ou neuf mois.

L'autre intérêt du hub réside dans ses capacités élastiques de calcul et de stockage – c'est la raison pour laquelle nous avons choisi une infrastructure *cloud*. À titre d'exemple, une clinicienne de l'AP-HP développe un projet d'aide au dépistage du cancer de la prostate qui mobilise le traitement de 10 000 imageries par résonance magnétique (IRM) par l'utilisation du *deep learning*. Elle travaille actuellement avec plusieurs établissements de santé mais aucun d'entre eux ne peut réunir au même endroit les 10 000 IRM et ne dispose des capacités de calcul et de stockage suffisantes pour appliquer les algorithmes – c'est pourquoi elle a eu recours aux services du hub.

Nous avons eu l'occasion de poser quelques jalons en 2020. Nous avons tout d'abord mis en production une plateforme pour des projets liés au COVID et avons procédé à sa mise à jour en fin d'année. Nous avons également conduit un second appel à projets au terme duquel nous avons sélectionné dix nouveaux projets sur le thème de l'intelligence artificielle et de la santé. Nous accompagnons aujourd'hui quarante projets : parmi eux, trente sont des projets pilotes et dix sont des projets liés au COVID – huit d'entre eux ont déjà reçu une autorisation de la CNIL et les deux derniers sont en attente de la recevoir. Nous animons des discussions avec les partenaires du catalogue ainsi que des actions de fédération de l'écosystème : un colloque, un *data challenge*, une *winter school* à laquelle 400 personnes se sont inscrites. Le hub rassemble aujourd'hui une cinquantaine de collaborateurs et nous formons l'ambition d'être soixante-dix en 2021. Enfin, nous sommes impliqués dans les travaux européens – j'y reviendrai.

Nous avons cinq priorités en 2021 :

– continuer la mise en place de la structure créée il y a un an ;

– industrialiser l'accompagnement des projets de bout en bout ;

– mettre en place des partenariats stratégiques et les développer, par exemple avec la CNAM, l'Institut national de la santé et de la recherche médicale (Inserm) et les établissements de santé ;

– associer le grand public au dispositif, en particulier compte tenu de la sensibilité des données ;

– enfin, développer l'infrastructure technologique.

Comment accéder aux données présentes dans le hub ? La réglementation française est très précise à ce sujet. Les porteurs de projets doivent constituer un dossier de demande d'autorisation d'accès aux données auprès de la CNIL. En la matière, le hub fait office de simple guichet administratif : le porteur de projet dépose son dossier au hub, qui le transmet à un comité éthique et scientifique national, qui vérifiera la solidité du projet tant du point de vue de la finalité poursuivie que de la méthodologie. Ce comité sera composé d'experts de très haut niveau, reliés à des experts extérieurs spécialistes de sujets très pointus. Si le comité accorde un avis favorable au dossier, le hub le transmettra à la CNIL. La CNIL est la seule autorité en mesure de délivrer ou non une autorisation de traitement de données. Le porteur de projet pourra ensuite s'adresser au hub en sa qualité de gestionnaire d'infrastructure afin qu'il mette à disposition les données, mais cela n'est pas obligatoire. Le porteur de projet doit être transparent sur l'objet de son étude, qui doit être décrite sur le site Internet du Health Data Hub et figurer au répertoire public disponible en ligne, ainsi que partager une partie des résultats de sa recherche.

Vous m'avez interrogée sur les articulations du Health Data Hub avec les initiatives locales, et en particulier avec le Ouest Data Hub. Nous conduisons un projet pilote avec le groupement de coopération sanitaire des hôpitaux universitaires du Grand Ouest (HUGO) qui porte le projet du Ouest Data Hub. Le Pr Marc Cuggia, impliqué dans ce projet, a participé à la mission de préfiguration du Health Data Hub. La convergence entre les initiatives a donc été imaginée dès le départ. Il n'est absolument pas dans l'intérêt du Health Data Hub de remplacer les initiatives locales : au contraire, il faut bien plus d'entrepôts de données hospitalières qu'il n'en existe aujourd'hui. Nous souhaitons permettre le passage à l'échelle par le développement de projets d'envergure nationale et le croisement des données.

Le projet que nous conduisons avec HUGO s'appelle Hugo-Share. Il vise à analyser les trajectoires médicamenteuses de 420 000 patients afin de comprendre et d'éviter les accidents iatrogéniques en ville et à l'hôpital et afin d'améliorer les parcours de soins des patients les plus fragiles, notamment les personnes âgées. Le Health Data Hub cofinance le projet et accueille la base chaînée au sein de la plateforme. La base clinique, elle, est fournie par le Ouest Data Hub et ses six établissements partenaires. Nous menons d'autres partenariats de ce type avec d'autres acteurs : par exemple, avec la Fédération nationale des centres de lutte contre le cancer (Unicancer) afin de mutualiser les données et de construire une base oncologique d'envergure, dans le respect de la réglementation et du droit des patients.

Vous m'avez également interrogée sur les raisons d'être et le rôle de la direction citoyenne. Son rôle s'articule autour de l'obligation légale du hub : informer les patients, promouvoir et faciliter leurs droits. La direction citoyenne ne remplace pas la direction

juridique. Nous identifions un enjeu à « embarquer » avec nous la société civile : il ne s'agit pas seulement d'informer les citoyens, mais de faire d'eux des partenaires du dispositif.

Cette direction anime quatre actions. La première consiste à étudier, consulter et concerter avec la société civile : nous constituons des groupes de travail afin de comprendre les attentes de la société civile et de recueillir sa perception du partage des données de santé. Nous sommes très impliqués dans l'action conjointe de la Commission européenne afin de mettre en place un espace commun de données de santé : le hub est l'autorité française compétente pour coordonner le travail des acteurs français sur le sujet. Ainsi, nous sommes chargés d'un lot de travaux relatif à l'infrastructure (cela concerne GAIA-X) ainsi que d'un lot de travaux sur l'engagement. Dans ce dernier lot de travaux, nous mettons en place une e-consultation pour nous adresser très largement à la société civile.

Nous cherchons également à mettre en place des partenariats concrets : par exemple, les associations de patients peuvent être autorisées à traiter des données. Nous avons ainsi conduit un premier partenariat avec France Asso Santé autour de l'étude intitulée « Vivre COVID », afin d'étudier comment les patients chroniques vivaient le premier confinement. Dans ce cas de figure, le hub apporte son appui à l'association de patients qui réalise l'étude et apporte ses données. Nous étudions actuellement comment le hub pourrait faire des requêtes au nom des citoyens ou des associations, quand ceux-ci ne sont pas en mesure de le faire eux-mêmes.

Il est également essentiel d'informer et de vulgariser, car la donnée de santé est particulièrement abstraite et complexe. Nous mettons en place des baromètres pour évaluer la connaissance ainsi que des outils de communication les plus vulgarisés possibles. Nous avons déjà produit deux vidéos et rédigé une note d'engagement avec un groupe de travail de patients. Nous souhaitons construire un contenu facile à lire et à comprendre sur le site Internet, afin de le rendre accessible au plus grand nombre de personnes. Cela pose évidemment de nombreuses questions sur l'exercice des droits, et ouvre également un chantier technologique sur la mise en œuvre des droits.

La direction citoyenne recouvre enfin une dimension de formation. Nous sommes actuellement en discussion avec l'Éducation nationale afin de mettre en place des outils de vulgarisation.

La fin de ma présentation porte sur le sujet qui, je pense, vous intéresse principalement : la sécurité et la souveraineté de la plateforme technologique. Je souhaite revenir sur les étapes qui nous ont amenées à choisir Microsoft et vous détailler où nous nous situons aujourd'hui au regard des décisions prises.

À l'été 2018, la ministre de la santé confie à la direction de la recherche, des études, de l'évaluation et des statistiques (DRESS) la feuille de route élaborée lors de la mission de préfiguration. À cette occasion, nous avons rencontré énormément d'acteurs : principalement des industriels français et des acteurs du monde de la recherche. Nous avons ensuite élargi notre champ, puisque nous nous sommes rendus compte que nos exigences étaient assez élevées. La première de nos exigences était la sécurité – cela n'a pas été tout de suite compris dans les débats qui ont eu lieu l'année dernière. D'aucuns pensent que nous avons choisi Microsoft en raison de ses capacités de *machine learning* ; en réalité, nous avons choisi Microsoft pour les services managés de sécurité. Il est extrêmement important de comprendre cela. Il n'existe aucun niveau équivalent dans l'industrie française en matière de services managés de cybersécurité, de ségrégation des droits, de gestion des droits, de traçabilité totale des activités de la plateforme. Or c'est cela que nous recherchions spécifiquement. Nous n'avons pas décidé nous-même de ces exigences de sécurité. Celles-ci sont réglementaires :

elles sont issues du référentiel de sécurité du Système national des données de santé, qui est très peu connu du grand public. La plupart des gens connaissent la certification des hébergeurs de données de santé (HDS), qui n'est pas obligatoire dans notre cas, mais bienvenue. C'est bien le référentiel de sécurité du SNDS qui est « incontournable » et qui constitue une exigence légale.

Nous avions également des exigences de performance : comme il ressort des exemples que j'ai précédemment donnés, nous souhaitons pouvoir croiser beaucoup de données et faire tourner du *deep learning* sur des IRM en masse, par exemple. Nous devons donc avoir une capacité à *scaler*, c'est-à-dire disposer d'une infrastructure capable de changer de taille en fonction des projets. C'est ce que le *cloud* nous permet de faire.

Enfin, nous posions une exigence de délai. Ce projet ne peut pas attendre : nous devons développer les usages numériques en santé et la crise a conduit, je crois, à une prise de conscience générale à ce sujet.

Nous avons ainsi choisi la solution de Microsoft, qui était la seule à répondre à toutes ces exigences. Il faut bien comprendre que notre plateforme n'est pas confiée à Microsoft : nous avons choisi le logiciel Azure de Microsoft, et Microsoft est, à ce titre, l'un de nos partenaires technologiques. Nous travaillons avec une dizaine de partenaires technologiques : la start-up française de cybersécurité Wallix, par exemple, nous fournit le bastion. Le Health Data Hub est souvent résumé à Microsoft ; mais nous n'avons pas demandé à Microsoft de construire une plateforme pour répondre à nos besoins. Microsoft est l'un de nos partenaires technologiques. L'un de nos plus gros partenaires technologiques est, d'ailleurs, la société française Open, qui est notre intégrateur.

Nous avons, dès le départ, posé la réversibilité de la plateforme comme l'une de nos exigences. Cela aurait été le cas même si nous n'avions pas eu recours à Microsoft. La réversibilité est indispensable. Dans tous les cas, il ne faut pas se retrouver piéger dans une solution technologique. Nous développons la plateforme en infrastructure *as Code*, c'est-à-dire programmable : nous essayons de disposer de scripts et de faire le moins d'actions manuelles possible. Nous pourrons alors, le moment venu, réutiliser les programmes informatiques : nous devrons alors les reparamétrer en partie, évidemment, mais une grande partie du travail sera réutilisable – c'est ce que l'on appelle la réversibilité.

Qu'avons-nous réalisé en faveur de la réversibilité, hormis cette automatisation ? Nous avons conduit deux études de réversibilité à ce jour. Cette exigence de réversibilité est inscrite dans la feuille de route et partagée par tous les acteurs partenaires du groupement d'intérêt public. À la fin de l'année 2019, nous avons publié notre première étude qui comparait l'acteur français OVH avec Microsoft et identifiait un écart important entre les deux. En juin 2020, nous avons mis à jour cette étude avec la direction interministérielle du numérique (DINUM). Nous avons alors identifié les quatorze besoins indispensables de la plateforme. Pour le moment, OVH n'en couvre que cinq. Ceci étant dit, nous n'avons aucun doute sur le fait que les acteurs français ont mis au point des feuilles de route très ambitieuses et vont progressivement réduire cet écart.

La souveraineté est un objectif pour chacun d'entre nous. Nous devons, nous, combiner cet objectif avec d'autres : ainsi, notre objectif prioritaire est de servir les patients. Les mesures de sécurité que nous avons mises en place ont été approuvées. Le débat ouvert aujourd'hui sur la souveraineté de la plateforme ne concerne donc pas la sécurité. Les données sont pseudonymisées et chiffrées. Nous avons recours à énormément de services de cybersécurité. Nous avons fait réaliser plusieurs audits par des prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés par l'ANSSI. Un audit de l'ANSSI est actuellement en cours.

Nous avons reçu un avis de la DINUM, un considérant du Conseil d'État dans son ordonnance a souligné le haut niveau de sécurité de la plateforme. La CNIL a déjà autorisé huit projets. Il est maintenant clair que la plateforme a atteint un très haut niveau de sécurité. Cela n'empêche cependant pas de poursuivre un objectif de souveraineté ; la difficulté est de savoir quels objectifs se cachent derrière la notion de souveraineté. Cela n'est pas clair pour l'instant.

Nous identifions actuellement des financements dans le cadre de France Relance, et menons des discussions avancées avec l'ANSSI pour construire une plateforme souveraine qui pourrait être la cible de la migration que vous évoquiez. Nous sommes très impliqués dans l'action conjointe de la Commission européenne, qui a été lancée le 1er février et devrait durer deux ans. Le lot de travaux concernant l'infrastructure pourrait faire le lien avec GAIA-X. L'initiative French Gaia-X Hub, quant à elle, a été lancée il y a quelques semaines : elle met en place des groupes de travail thématiques et nous participons notamment au groupe de travail des « utilisateurs santé ». Nous souhaitons travailler collectivement à construire une solution plus souveraine, tout en gardant en tête que le Health Data Hub n'est pas nécessairement la seule dimension d'un espace commun de données de santé à l'échelle européenne.

Par ailleurs, et pendant ce temps, nous continuons nos échanges très réguliers avec les différents acteurs de la filière. Nous avons récemment conduit un premier échange au sujet de la solution Anthos avec OVH et Google. Nous continuons donc évidemment à suivre l'évolution du marché.

M. Philippe Latombe, rapporteur. Vous avez souligné, à la fin de votre intervention, le haut niveau de sécurité du dispositif et indiqué que la souveraineté était une autre question. Vous avez alors fait remarquer que la définition de la souveraineté n'était pas claire. Que signifie, selon vous, la souveraineté ?

Mme Stéphanie Combes. Je ne suis pas compétente moi-même pour la définir, mais les discussions que nous avons pu avoir au sujet du Health Data Hub font ressortir un enjeu d'autonomie stratégique. Il s'agit de savoir si l'on est en situation de dépendance et si nous pouvons nous assurer que les données puissent être à tout moment récupérées. Cette notion recouvre également un enjeu lié aux lois extraterritoriales, s'agissant des hébergeurs de *cloud* américains. La question des lois extraterritoriales est assez technique – plusieurs sont mises en avant, dont le *Cloud Act* américain – et il convient d'étudier le sujet de manière assez fine. Ces lois s'appliquent dans certains contextes, qui ne sont pas forcément valables pour tous les hébergements de toutes les données personnelles. Dans le cas du hub, les données sont pseudonymisées.

Se posent également des questions de filières. Nous pourrions souhaiter soutenir le plus possible les acteurs de la filière française – d'autant plus que le projet est porté par l'État. Cela crée des injonctions parfois contradictoires : l'État porte un projet, donc il ne souhaite travailler qu'avec des acteurs français ; en même temps, l'État nous demande d'être rapides et d'avoir des résultats concrets.

Il faut vraiment traiter cette question de la souveraineté – mais je ne pense pas être la personne pour le faire. Ma crainte serait qu'elle ne soit pas complètement traitée, c'est-à-dire que l'on n'atteigne pas une définition conceptuelle claire, et que cela ait un impact non maîtrisé sur l'écosystème. On parle de loi extraterritoriale – mais parle-t-on des actionnaires étrangers ? Tous ces critères doivent être élaborés et partagés, et nous devons nous mettre d'accord sur la cible. Sinon, nous allons mettre en place des critères extrêmement restrictifs et nous allons supprimer des usages.

J'ai une seconde crainte. J'entends beaucoup parler du *cloud* et de Microsoft, mais je n'entends pas beaucoup parler de la souveraineté des usages numériques de santé. Dans certains autres pays, et notamment aux États-Unis, ces questions avancent très vite. En mai 2018, le dispositif médical pour les examens de fond d'œil était le premier dispositif médical intégrant l'intelligence artificielle à être autorisé par la *Food and drug administration* (FDA). Cela a constitué une très belle avancée et depuis, une trentaine d'autres dispositifs médicaux ont été autorisés par la FDA. Nous téléchargerons bientôt toutes ces applications sur nos téléphones, car elles proposeront des usages de santé extrêmement intéressants et performants ; mais elles n'auront pas été construites grâce à des données de patients français et l'on ne saura même pas si elles ont été développées dans le respect du Règlement général sur la protection des données (RGPD). Il faut donc garder en tête les questions sur la souveraineté des usages, afin de ne pas nous retrouver dans cinq ans à discuter de ces mêmes sujets car nous aurons pris du retard par rapport à d'autres acteurs. Il faut donc procéder à des arbitrages en ayant bien en tête tous les enjeux ayant cours au même moment. Cela n'est pas simple.

M. Philippe Latombe, rapporteur. Les critiques ne portent pas sur le fond du projet du Health Data Hub ni sur les objectifs qu'il poursuit. Elles visent, de façon très claire, l'hébergement dans le *cloud* d'Azure de Microsoft. Ces critiques sont présentes quasiment depuis le lancement du projet. Comment les appréhendez-vous et comment les intégrez-vous à votre démarche ? Vous avez insisté sur le fait que Health Data Hub devait être développé rapidement. Ces critiques ne constituent-elles justement pas un frein à son développement ? Je pense notamment à la procédure lancée devant le Conseil d'État, à la réticence de la CNAM quant au transfert de ses données, à l'expression permanente de critiques de la part de l'écosystème, à l'intervention du secrétaire d'État chargé du numérique devant le Sénat pour évoquer la réversibilité. Quels sentiments ces critiques suscitent-elles chez vous ?

Mme Stéphanie Combes. Il faut prendre les critiques de manière précise. Quand j'ai commencé à conduire le projet, on a critiqué sa lenteur annoncée, en prédisant que le Health Data Hub connaîtrait le même destin que le dossier médical partagé (DMP). Si j'avais choisi une solution qui n'aurait pas aujourd'hui permis au projet d'aboutir, je serais également critiquée. En tant que chef de projet d'un projet d'État, je suis assez à l'aise avec l'idée d'être critiquée. On ne va pas encore assez vite, je vous l'accorde – mais nous n'aurions même pas encore esquissé le début d'une plateforme si nous avions opté pour une autre solution.

Il faut donc prendre les critiques, étudier où elles prennent leurs sources et les traiter. Certaines critiques relèvent d'un problème de compréhension technologique – il faut donc faire de la vulgarisation. Il est vrai que l'État et les activités publiques sont moins à l'aise avec les solutions de *cloud* que le secteur privé. La DINUM travaille sur ces sujets, notamment en élaborant une stratégie *cloud* souveraine. Nous nous inscrivons dans cette dynamique.

Le conseil de la CNAM ne représente pas à lui seul l'ensemble de la CNAM. Le conseil de la CNAM ne s'est pas exprimé seulement sur Microsoft : il a également critiqué le décret, qu'il a jugé incompréhensible. Il faut étudier l'origine du problème et le traiter. La mise en place des dispositifs de *cloud* relève de la conduite du changement ; ce projet est très différent des choix opérés par l'Assurance maladie depuis des dizaines d'années. Nous devons donc accompagner ce mouvement.

Les critiques proviennent souvent de l'écosystème du numérique français. Les acteurs du numérique français trouvent injuste que nous ayons opté pour Microsoft comme opérateur d'un projet public. Je comprends cette critique, mais si nous avions opté pour un autre partenaire que Microsoft, certains autres acteurs encore auraient été mécontents. On ne pourra

jamais satisfaire tous les prestataires industriels. Nous sommes confrontés au jeu de la construction et de la sélection des partenaires technologiques.

Une autre critique provient du monde hospitalier, qui me semble pouvoir être traitée par la preuve. Le secteur hospitalier craint que le Health Data Hub cherche à remplacer ses activités. Il est intéressant, à ce sujet, d'étudier l'historique des critiques formulées par l'association InterHop et de savoir qui a fondé cette association. Il s'agit de deux anciens personnels de l'entrepôt de données de santé de l'AP-HP : leur propos premier était d'affirmer qu'il n'était pas besoin de mettre au point le Health Data Hub car la solution de l'AP-HP existait déjà. Nous sommes parfaitement d'accord avec l'idée selon laquelle il ne faut pas centraliser et il ne faut pas tuer les activités locales : nous n'allons pas remplacer le travail de l'Assurance maladie, ni celui de l'entrepôt de données de l'AP-HP. Ils fournissent un travail énorme, que nous respectons et que nous voulons soutenir. L'association InterHop utilise aujourd'hui l'argument du logiciel libre. Nous n'avons pour le moment pas bien compris quels éléments ils ont versé en *open source*.

Il faut donc identifier chaque source de critique, étudier comment la traiter et apporter tous les éléments de preuves qui nous sont demandés. C'est de cette manière que nous pourrons conduire l'innovation : à ce titre, le Health Data Hub est loin d'être le premier projet à souffrir la critique.

M. Philippe Latombe, rapporteur. N'avez-vous pas l'impression que les critiques, qui sont apparues dès le début du projet, entravent vos activités – qu'elles sont en quelque sorte devenues un boulet ? J'en veux pour preuve la réversibilité, qui a été l'une des conséquences de ces critiques.

Mme Stéphanie Combes. Non, la réversibilité a été identifiée dès le premier jour.

M. Philippe Latombe, rapporteur. Je l'ai bien compris. Cette réversibilité, cependant, est aujourd'hui prévue à deux ans.

Mme Stéphanie Combes. Le courrier du ministre diffusé dans la presse ne mentionne pas la migration, mais l'annulation du risque extraterritorial. Nous travaillons, ensuite, dans un objectif de souveraineté, car cet objectif est poursuivi par l'ensemble des services de l'État. Il faut étudier les sujets précisément. Vous pouvez, si vous voulez, évoquer un boulet : je préfère parler d'agilité. Si l'on avait procédé différemment, aucun projet n'aurait été conduit sur le hub aujourd'hui et aucun d'entre eux ne produirait des résultats dès cette année. Disposer d'une cible industrielle conforme à d'autres ambitions que celles d'abord exprimées par la ministre, auxquelles je souscris entièrement, d'avoir des résultats rapides représente une progression et ouvre de nouveaux chantiers. Il s'agit d'un projet extrêmement ambitieux, il est donc normal que nous ayons plusieurs étapes de réalisation – cette étape d'infrastructure souveraine en fait partie.

M. Philippe Latombe, rapporteur. Pensez-vous que le projet aurait été mené plus rapidement sans ces critiques de départ ?

Mme Stéphanie Combes. Non. Cela n'a pas de lien avec la question de la parution du décret. L'impact de la crise sanitaire sur le ministère suffirait à l'expliquer. En revanche, le ministère a été très réactif sur l'arrêté qui nous a permis de préfigurer le catalogue avec les données du COVID. Je ne crois donc pas que nous aurions pu faire plus vite en procédant différemment.

L'étude de réversibilité conduite l'été dernier avec la DINUM montre qu'OVH, le leader français dans le domaine, ne satisfait toujours pas nos prérequis. Nous serions donc encore aujourd'hui en train de construire une solution.

M. Philippe Latombe, rapporteur. Je voudrais que les choses soient claires. Comment s'est déroulé le processus de sélection au tout départ ? Avez-vous lancé un appel d'offres ? Si oui, quels en étaient les critères ? Quelles entreprises ont été autorisées à y répondre ? Beaucoup de critiques portent également sur la phase de démarrage du projet.

Mme Stéphanie Combes. Il n'y a pas eu d'appel d'offres. Nous avons recours aux services de l'union des groupements d'achats publics (UGAP). Tout comme la centrale d'achat de l'informatique hospitalière (CAIH) ou le réseau des acheteurs hospitaliers (Resah), l'UGAP est une centrale d'achat mise en œuvre pour faciliter l'achat public. Ces structures mettent elles-mêmes en concurrence les acteurs, conçoivent un catalogue dans lequel nous pouvons choisir. Il ne s'agit donc pas d'un contournement du code des marchés publics. La mise en concurrence a été faite, mais non ciblée sur notre projet. Nous nous appuyons donc sur l'UGAP. Nous sommes aujourd'hui une petite structure de 50 personnes, qui n'est pas en capacité de porter un marché de 200 millions d'euros.

Le ministère de la santé a élaboré à l'époque les prérequis : ceux-ci relèvent à la fois du juridique et de la cybersécurité. Nous avons rencontré les industriels et les avons interrogés, à chaque fois, sur le référentiel de sécurité du SNDS, qui est différent de la certification HDS. Le prérequis HDS était également important pour nous : nous n'envisagions pas de sélectionner une structure qui ne soit pas certifiée HDS. Enfin, les prérequis demandés concernaient les fonctionnalités, puisque nous souhaitions mettre en place une plateforme dotée de capacités de calcul et de stockage élastiques. Un document, résumant tous ces prérequis, a été rendu public sur le site de la direction de la recherche, des études, de l'évaluation et des statistiques (DRESS).

Nous avons par ailleurs conduit des échanges bilatéraux avec tous les industriels de l'écosystème français déjà évoqués – Atos, Thales, OutScale, CASD, TeraLab – pour étudier leurs offres. La première étude de réversibilité cote la présence, ou non, des certifications ou des fonctionnalités chez chacun des acteurs. Ces résultats auraient pu être « challengés » par les acteurs, mais cela n'a pas été fait – et pour cause, seul Microsoft était habilité HDS à l'époque. Cela est vrai et vous pouvez le vérifier. Nous avons donc conduit la comparaison, puis nous avons vérifié qu'Open, notre intégrateur, et Microsoft étaient tous deux disponibles au catalogue de l'UGAP. Cette manière de procéder est légale, et plus encore, elle est recommandée par la DINUM. Le mécanisme de centrales d'achat a été mis en place pour faciliter l'achat public.

M. Philippe Latombe, rapporteur. Nous avons auditionné l'UGAP et la DINUM. La DINUM nous a expliqué que les achats étaient aussi guidés par le besoin de facilité : les administrations achètent des solutions totalement intégrées car elles n'ont pas les moyens d'intégrer ensemble des blocs différents pour constituer une solution complète. Ce souci de facilité et de rapidité explique-t-il que vous ayez également choisi Microsoft ?

Mme Stéphanie Combes. Je ne parlerais pas de simplicité – je ne dirais pas que notre chantier d'infrastructure est simple. Nous avons choisi une solution qui répondait à notre demande, alors que les acteurs français ne proposaient pas les fonctionnalités dont nous avions besoin. Il aurait fallu construire ces fonctionnalités et cela aurait pris un certain temps. Encore aujourd'hui, OVH n'a pas développé toutes ces fonctionnalités.

M. Philippe Latombe, rapporteur. On aurait pu envisager un consortium : plusieurs acteurs auraient pu travailler ensemble pour apporter ces différentes fonctionnalités.

Mme Stéphanie Combes. Si nous avions publié un marché public, Microsoft y aurait répondu. On ne peut pas choisir de travailler avec un acteur français car on a envie de soutenir son développement industriel, si un autre acteur répond à notre demande, dispose de toutes les certifications requises et mène une activité sur le sol de l'Union européenne. On ne peut pas interdire à des acteurs internationaux de fournir des services. Si demain il existe une nouvelle certification, que Microsoft ne la vérifie pas et qu'OVH la vérifie, alors les choses seront différentes. À l'époque, si nous avions publié un marché, Microsoft l'aurait remporté. Il a même été proposé, pour apaiser le débat, de publier un marché *a posteriori* : c'est à nouveau Microsoft qui aurait été choisi et cela n'aurait fait que jeter de l'huile sur le feu. Il nous manque, collectivement, un *benchmark* du niveau de maturité des solutions de *cloud* françaises endossé par l'État. Il faudrait que ce *benchmark* soit conduit par le ministère de l'industrie ou bien par la DINUM. Cela nous permettrait d'attester collectivement du fait que des acteurs français sont très forts dans tel domaine, et plus faibles dans d'autres. Cela traduirait la réalité du terrain.

M. Philippe Latombe, rapporteur. Je peux le comprendre, et je n'ai pas de critique à y apporter. Je reviens sur ma question du boulet. Les critiques initiales ont marqué le Health Data Hub du sceau d'une réelle difficulté. On évoque aujourd'hui le hub bien davantage pour ces critiques que pour ses succès. Il a été annoncé qu'il faudra migrer vers une solution souveraine et que cela prendra deux ans. Cela donne l'impression qu'une décision prise nous lie pendant des années et que la réversibilité n'est pas si simple que cela à mettre en œuvre. Cette situation jette l'opprobre sur le projet.

Mme Stéphanie Combes. Pour mettre en œuvre la réversibilité, il faut que la cible soit prête. La cible n'est pas prête pour le moment, il faut donc prendre le temps de la construire. Cela n'est pas la faute du hub. De notre côté, la migration nous prendra quelques mois. La CNIL en avait parfaitement conscience. Tout le monde est d'accord sur le fait qu'il est souhaitable que l'hébergement soit souverain – il faut se donner les moyens d'y arriver, et pour cela, il faut donc le temps à l'industrie de développer la solution cible. Cela explique la durée de deux ans.

Nous avons, par ailleurs, en France, un problème avec le numérique. Par faute de compréhension de ses enjeux très techniques et de manque d'ingénieurs dans les administrations, tout le monde donne son avis sur des sujets d'une complexité très importante. Nous ne pouvons pas remettre en cause des choix technologiques : nous avons travaillé à l'infrastructure technologique sécurisée avec le haut fonctionnaire de défense et de sécurité du ministère de la santé et avec l'ANSSI, qui est la plus haute autorité en la matière en France. Nous avons collectivement besoin d'éduquer les Français sur cette composante numérique qui va être de plus en plus présente dans nos vies, afin de conduire des débats moins passionnels et plus objectifs. Cela rejoint la question de la souveraineté que vous me posiez plus tôt : tout le monde parle de la souveraineté numérique, mais sa définition n'existe pas. Cela est un vrai problème.

Il est vrai que depuis sa création, la communication du hub tournait surtout autour de la plateforme technologique et de ses critiques. Nous commençons cependant maintenant à produire des résultats ; cela est de nature à davantage montrer la finalité du Health Data Hub. L'intérêt de notre action et ses vrais usages seront bientôt visibles : le développement des outils à destination des professionnels et des patients, la recherche médicale, les outils de prédiction des ré-hospitalisations. Mais notre action appartient à la recherche, cela prend donc du temps.

M. Philippe Latombe, rapporteur. S'agissant des coûts, il nous a été expliqué que des différences tarifaires assez fortes peuvent exister entre les différents fournisseurs. Comment se situe Microsoft en la matière ? Était-il significativement moins cher que les autres fournisseurs, de manière à « acheter le marché » ? Ou était-il au contraire plus cher car il se savait être le seul fournisseur à répondre au cahier des charges ?

Ensuite, Microsoft vous a-t-il imposé de négocier toutes les conditions générales d'utilisation et les conditions particulières au sein du contrat ?

Enfin, il nous a été dit que l'envoi des données sur le *cloud* de Microsoft était relativement peu cher, mais que la sortie était extraordinairement chère. Avez-vous pris en compte ce critère et si oui, avez-vous pu le négocier ?

Mme Stéphanie Combes. S'agissant des coûts, la centrale d'achat met en compétition les acteurs en intégrant un critère de coût. Nous avons comparé le coût entre OVH et Microsoft lors de notre première étude de réversibilité. La comparaison a montré qu'il était beaucoup moins cher de construire l'infrastructure Microsoft – car elle est tout intégrée – mais qu'à l'usage, elle est un peu plus chère.

Nous avons évidemment également étudié les conditions de sortie des données. Cet argument était très valide, il y a quelques années, mais il l'est beaucoup moins aujourd'hui. Les acteurs ne sont plus dans la logique de capter les utilisateurs par le coût de sortie des données, car les utilisateurs y sont désormais vigilants. Les acteurs américains vont plutôt développer des services de plus en plus intelligents, ergonomiques, de haut niveau, pour capter l'utilisateur car ils n'ont pas d'équivalents. Ainsi, nous n'utilisons ainsi pas d'outils intégrés de *machine learning,* nous mettons à disposition des outils très standard de *data science* en *open source* comme R et Python.

Nous avons en effet négocié plusieurs avenants aux clauses de contrat ; cela s'est fait au fur et à mesure de nos discussions notamment avec la CNIL. Nous en avons négocié trois au total et nous continuerons d'en négocier si cela est nécessaire.

M. Éric Bothorel. Notre mission sur la souveraineté numérique fonctionne sur Zoom et je constate que la totalité de nos données n'est pas chiffrée.

Je me souviens des débats ayant eu lieu au printemps sur l'application StopCovid, aujourd'hui Tous anti-Covid. Les choix opérés sont systématiquement critiqués. Cela est probablement le cas pour de bonnes raisons, car des subtilités technologiques vont parfois à l'encontre de notre autonomie stratégique.

Il était question tout à l'heure de chiffrement. Qui stocke les clés de chiffrement ? Cela constitue une garantie de la protection des données stockées sur le Health Data Hub.

Le Health Data Hub fait-il l'objet de cyberattaques actuellement ? Si oui, connaît-on la nature et l'origine de ces tentatives ? Je souhaiterais savoir comment le Health Data Hub s'organise pour faire face à la sphère cybercriminelle qui pourrait être tentée d'accéder à ses données et quelles sont les mesures déployées pour l'en empêcher.

Mme Stéphanie Combes. Les données sont toutes chiffrées, à la fois lorsqu'elles sont stockées et lorsqu'elles se déplacent. Les clés sont stockées dans des modules numériques appelés *hardware security modules* (HSM), qui constituent le plus haut niveau de sécurité internationale. Nous créons des clés dites maîtresses à l'extérieur de la plateforme dans un HSM maîtrisé par le ministère. Elles sont ensuite envoyées à l'intérieur de HSM de Microsoft,

car la clé doit se trouver à l'intérieur de la plateforme pour y chiffrer et déchiffrer les données. Le HSM ne nécessite aucune intervention d'un administrateur de Microsoft ni même du hub : cela constitue une norme de sécurité internationale. Le fait que nous possédions les clés maîtresses nous permet, si nous le souhaitions, de révoquer les clés en cas d'accident majeur et donc de supprimer les données (qui ne sont que des copies, puisqu'il s'agit de données de recherche). Les avenants au contrat prévoient bien que Microsoft ne cherchera jamais à contourner ce chiffrement ou à récupérer des clés de chiffrement pour les confier à un tiers.

Le Health Data Hub n'a pas aujourd'hui fait l'objet de cyberattaques. Cela constitue d'ailleurs l'un des indicateurs de notre stratégie pluriannuelle de transparence envers notre assemblée générale. Si nous sommes informés d'une cyberattaque, les analystes de mon équipe RSSI examinent si nous sommes concernés et instruisent la cyberattaque. Nous organisons par ailleurs des « attaques » de manière volontaire pour tester la plateforme : nous en avons déjà mené deux et un troisième audit est actuellement en cours avec l'ANSSI.

M. Philippe Latombe, rapporteur. Vous avez expliqué tout à l'heure que le hub n'était pas exclusif d'initiatives locales. Ainsi l'AP-HP disposait déjà d'une plateforme technologique et d'un entrepôt de données. Pourquoi ne pas avoir utilisé l'architecture du dispositif de l'AP-HP pour le faire grossir ? Pourquoi avoir fait le choix d'une solution technologique différente ?

Mme Stéphanie Combes. Nous avons évidemment envisagé cette option et nous avons eu l'occasion d'échanger à plusieurs reprises avec le DSI de l'AP-HP à ce sujet. L'AP-HP est l'acteur français le plus avancé en matière d'entrepôt de données hospitalières. Leur travail est formidable. Pour le moment, leur solution n'est pas conforme au référentiel de sécurité du SNDS – or cela constituait une obligation légale pour le hub. Par ailleurs, leur infrastructure sur site ne leur permet pas de passer à l'échelle pour tout type de projet, comme nous pouvons le faire avec une infrastructure *cloud*. Nous menons actuellement des projets en partenariat, qui montrent bien la complémentarité de nos solutions technologiques : l'AP-HP commence le projet avec d'autres partenaires, et nous arrivons en bout de chaîne par le traitement algorithmique en apportant la capacité de calcul nécessaire.

M. Philippe Latombe, rapporteur. Y'a-t-il eu de l'entrisme de la part de Microsoft auprès du Health Data Hub ? Existe-t-il des liens, des connexions – y compris amicales – entre des personnes du Health Data Hub et Microsoft ? Ces propos sont revenus fortement sur les réseaux sociaux. L'on parle beaucoup de mobilités de personnels entre les prestataires et l'administration. Est-ce l'une de vos préoccupations ? Avez-vous pu vérifier ce type de mouvements qui pourraient poser, à terme, des questions d'éthique et de déontologie ?

Mme Stéphanie Combes. Nous n'avons aucun lien, à l'origine, avec Microsoft. Je suis ingénieure utilisatrice de données et j'ai eu l'occasion d'utiliser entre autres les solutions de Microsoft Azure et d'Amazon Web Services (AWS) par le passé. Je ne connaissais absolument pas les personnes de Microsoft avec lesquelles je travaille aujourd'hui. L'équipe technique aujourd'hui présente au hub n'existait d'ailleurs pas lors du lancement du projet. Je suis administratrice de l'INSEE et s'agissant du choix des partenaires technologiques, j'ai d'abord pensé à TeraLab et au centre d'accès sécurisé aux données (CASD) qui sont les acteurs de la statistique publique. Nous nous sommes tournés vers les solutions américaines très tardivement. Nous avons élargi nos recherches lorsque nous nous sommes rendus compte que les acteurs n'étaient pas en mesure de répondre à notre cahier des charges. Nous avions un vrai problème si nous n'étions pas capables de mettre en place une plateforme de *data science* en santé avec des outils sur étagère. En fin de course seulement donc, nous avons commencé à interroger Microsoft, AWS et Google Platform. Je vous garantis que le choix de Microsoft n'a pas été un choix d'influence. Je suis ingénieur. Nous avons été pragmatiques et nous avons

souhaité obtenir une solution rapide dans un contexte dans lequel la France n'est pas en avance. La législation française et européenne est très forte : cela est positif, mais cela constitue également une complexité – réaliser des projets sur des données de santé en France est complexe. Le choix de Microsoft n'a pas été un choix d'influence mais, la crise sanitaire l'a montré, l'écosystème français de la recherche en santé est confronté à plusieurs autres problèmes.

M. Philippe Latombe, rapporteur. Comment avez-vous analysé l'arrêt *Schrems* II, lorsqu'il a été rendu ? Maintenant que les conséquences de cet arrêt ont été formulées et que l'on vous a demandé de migrer vers un *cloud* souverain, où en êtes-vous de ce travail ?

Mme Stéphanie Combes. Il est intéressant que vous reliiez ces deux questions car, à mes yeux, il n'existe pas tellement de rapport entre elles.

L'arrêt *Schrems* II porte sur le transfert de données personnelles. Pendant toute la première moitié de l'année 2020, notre effort de pédagogie lors des débats sur le Health Data Hub a consisté à expliquer qu'il n'y avait pas de transfert de données de santé. D'aucuns affirmaient alors que les données étaient hébergées aux Pays-Bas puis traitées aux États-Unis – cela est un non-sens du point de vue technologique. Nous avons mis un certain temps à convaincre et à montrer, avenant à l'appui, que les administrateurs de Microsoft n'accédaient jamais aux données et que les services d'utilisation des données étaient également régionalisés. Nous avons réussi à documenter cela et à en convaincre la CNIL. Le Conseil d'État en a ensuite attesté en affirmant qu'il n'y a pas de transfert de données personnelles. En revanche, Schrems II est un vrai problème pour les acteurs qui procèdent à des transferts de données, en raison des clauses contractuelles types et des mesures techniques et organisationnelles à mettre en place pour améliorer la sécurité des transferts de leurs données personnelles.

Les engagements pris en matière de souveraineté par M. Cédric O ou par le ministère de la santé sont fondés sur le risque extraterritorial, lequel n'a pas été reconnu par le Conseil d'État. La compréhension des lois extraterritoriales est donc problématique. Nous menons des travaux juridiques pour documenter l'impact des lois extraterritoriales ; nous identifions, avec la DINUM, nos services essentiels ; et enfin, nous recherchons des financements. Si nous créons demain cette plateforme, nous aurons besoin de financements. Nous avons identifié des financements dans le plan de relance – l'accélération de la stratégie du *cloud* souverain est portée par la direction générale des entreprises (DGE). Par ailleurs, nous participons aux projets européens et nous suivons toutes les activités de l'ANSSI autour de la cybersécurité dans le cadre du plan de relance. Je suis donc assez confiante dans notre capacité interministérielle à débloquer les 20 millions d'euros nécessaires au développement d'une solution souveraine. Évidemment, cette solution souveraine ne servirait alors pas qu'au Health Data Hub – l'enjeu d'une plateforme souveraine va concerner de nombreux autres *data hubs* dans beaucoup d'autres secteurs.

M. Philippe Latombe, rapporteur. C'est justement pour cela qu'il était important de vous recevoir – vous avez été précurseur en la matière s'agissant des données de santé et vous avez par conséquent essuyé toutes les critiques. Ces solutions de *data science* vont intéresser demain beaucoup d'autres domaines. Ne faudrait-il pas, de votre côté, accélérer autant que possible le développement du projet ? Disposez-vous du soutien financier et technique de l'État pour mener ce projet le plus vite possible ?

Mme Stéphanie Combes. Nous tenons depuis longtemps des discussions avec la DINUM, l'ANSSI, le Premier ministre, le ministère de la santé. Nous constatons un alignement avec la stratégie *cloud* de l'État et cela va permettre de concrétiser ces ambitions. En tant que chef de projet, j'identifie les fonds, car sans fonds, nous ne pourrions rien faire de

concret. Je suis aujourd'hui confiante en notre capacité à faire. En revanche, le délai est extrêmement ambitieux sur le plan industriel. Mais c'est en se fixant des objectifs ambitieux que nous réussirons à franchir des paliers.

M. Philippe Latombe, rapporteur. Comme vous l'avez dit, la solution souveraine intéressera de nombreux autres ministères et de nombreux autres sujets. Il serait sensé de construire une solution qui sera utilisable par l'ensemble des acteurs.

Que retenez-vous, depuis la création du Health Data Hub jusqu'à maintenant, des difficultés auxquelles vous avez été confrontée ? Comment voyez-vous les choses dans les mois et les années à venir ? Allez-vous réussir à faire la preuve d'une réversibilité qui fera oublier le démarrage du Health Data Hub ?

Mme Stéphanie Combes. Mener des projets et produire des résultats de recherche concrets va donner du sens à notre démarche. La critique adressée au Health Data Hub s'agissant de Microsoft intéresse l'écosystème du numérique français et les acteurs nourrissant des craintes sur la protection des données – ils peuvent être rassurés par les avis apportés par les autorités prescriptrices. Les gens comprendront pourquoi nous avons mis en place le Health Data Hub quand nous pourrons mettre en avant des résultats de recherche convaincants et concrets.

Les enjeux numériques, aujourd'hui extrêmement passionnels et mal compris, doivent être mis au second plan par rapport aux finalités que les plateformes poursuivent. Il en va exactement de même pour StopCovid : les gens se sont d'abord interrogés sur la manière dont cette application traiterait leurs données personnelles. Mais il faut surtout et avant tout se demander à quoi sert cette application. Nous devons, nous, tous les acteurs du numérique, travailler à rendre l'usage final très clair.

Nous continuerons donc à travailler sur le chantier de l'infrastructure et à produire des résultats. Un écosystème très enthousiaste nous suit, et regrette que notre développement soit trop lent ; nous recevons énormément de réponses à nos appels à projets ; nous enregistrons une très forte participation à nos événements fédérateurs comme le colloque, le *data challenge*, la *winter school*.

La vraie difficulté du Health Data Hub pour les prochaines années est ailleurs. Nous sommes face à un problème culturel de réflexe en ce qui concerne les données de santé. Les données de santé n'appartiennent à personne et personne ne le sait. Certains écosystèmes de santé et établissements pensent que les données leur appartiennent parce qu'ils ont fait l'effort de collecte et qu'ils ont soigné les patients. Les acteurs ne savent pas quand ils ont le droit ou non de traiter les données. Cela est extrêmement complexe et constitue un vrai frein à l'innovation en santé. Ainsi, certaines personnes ne respectent pas le cadre applicable et certaines autres personnes sont frileuses, car elles ne maîtrisent pas le cadre. Si nous ne cassons pas cette spirale, le Health Data Hub sera un prestataire d'outils de *data science* pour quelques projets et nous passerons à côté de l'ambition du dispositif.

Nous avons donc besoin d'un écosystème institutionnel autour de la donnée de santé, avec une politique nationale et des financements dédiés. Je citerai l'exemple de la *UK Bio Bank*, une base de donnée anglaise reconnue au niveau international et dont les données sont utilisables par tous. Les contributeurs à cette base n'ont aucun réflexe de propriétaire. Pourquoi ? Le financement de cette base est pérenne et ne dépend pas des publications des acteurs qui sont à l'origine de la base. Ainsi, n'émergent pas chez les acteurs des comportements pervers qui impliquent de réserver les données pour eux-mêmes car ils ont besoin des financements associés aux données. Le Plan national pour la science ouverte est

porté au plus haut niveau par le ministère de la recherche, mais il doit être associé à des dispositifs incitatifs : il n'est pas concevable, pour les chercheurs, d'ouvrir la science mais d'encore devoir lutter pour trouver des financements. Le hub peut porter mais ne peut pas être maître d'œuvre de cette politique de la science ouverte et de la santé – cela n'est pas notre rôle. À titre d'exemple, le Ségur du numérique ne prévoit pas d'enveloppe pour les données de santé de recherche – et ce, même à l'issue d'une crise sanitaire.

M. Philippe Latombe, rapporteur. Cela veut-il dire que le frein provient aussi de nos concitoyens, qui voient les données de santé comme une donnée sacrée, qu'on ne peut pas utiliser ni vendre ? Doit-on évoluer vers un modèle semblable à la *UK Bio Bank* ou bien au modèle israélien ? La nature même de la donnée de santé ne constitue-t-elle pas un frein ?

Mme Stéphanie Combes. C'est une question complexe à laquelle je ne saurais répondre de manière définitive, mais je n'en suis pas certaine. Nous avons mené plusieurs études de perception du partage des données de santé par les citoyens. Ils ne sont pas opposés à l'idée de partager leurs données de santé à des fins de recherche. Ils formulent seulement une crainte particulière quant à l'accès des assureurs aux données, et expriment une réserve supplémentaire au sujet de l'industrie pharmaceutique. La vente des données de santé est interdite par la loi française. La tarification de la mise à disposition des données, en revanche, est possible en France. Cela permettrait de tarifer la mise à disposition de données à un acteur privé afin d'investir dans la base de données. Cela est plutôt sain car investir dans une base de données est très coûteux.

À mes yeux, le sujet porte donc davantage sur l'écosystème : les acteurs qui collectent les données et se sentent insuffisamment valorisés pour ce travail. À ce titre, la politique pour la science ouverte vise à valoriser la production de données au même titre qu'une publication scientifique. Je viens du secteur de la statistique publique et je considère que la production de données est un métier essentiel. Dans l'écosystème de la recherche, au contraire, ce métier est connoté tout à fait négativement. Nous avons donc besoin de valoriser le *data sharing,* de financements pérennes pour les bases et que les personnes qui portent des cohortes ne soient pas inquiètes des financements pour les grandes cohortes essentielles.

M. Philippe Latombe, rapporteur. Comment les choses se passent-elles avec les bases locales, s'agissant notamment de la rémunération et du partage des coûts ?

Mme Stéphanie Combes. Nous avons mis en place une offre de services à destination des responsables de données, c'est-à-dire des acteurs à l'origine de la réunion des données. Nous avons travaillé avec des panels d'acteurs sur une convention-type qui encadre le partage. Deux articles ont nécessité un travail important.

Il s'agit tout d'abord d'un article sur la valorisation scientifique. Selon les recommandations internationales, une personne qui a contribué en apportant des données ne peut pas être signataire d'un article scientifique. Cela constitue un vrai problème, car être signataire permet de gagner des points qui donnent lieu à une rémunération. À ce sujet, nous avons réussi à trouver un compromis dont nous sommes assez satisfaits.

Le second article problématique portait sur la tarification : la question est de définir l'assiette possible de la tarification. Les bases publiques à finalité administrative ont, pour la plupart, toutes déjà été financées par des fonds publics. En revanche, les bases de recherche supposent la création d'une infrastructure pérenne, avec des équipes et des investissements technologiques importants, qui sont très coûteux. Les réflexions sont toujours en cours à ce sujet. La Commission européenne réfléchit en ce moment même, notamment avec la mise en place du *Data Governance Act* et la réflexion autour de l'espace commun des données de

santé. Le *Data Governance Act* prévoit un article sur la tarification et les mêmes questions vont émerger sur le point de savoir ce que doit recouvrir ce tarif.

M. Philippe Latombe, rapporteur. Nous avons souhaité cette audition car vous êtes précurseur des enjeux de souveraineté en matière de données de santé avec la création du Health Data Hub. L'utilisation d'un écosystème afin de créer un support pour toutes les *data science* est une idée. Je vous remercie pour ces échanges.

Mme Stéphanie Combes. N'hésitez pas à me dire si vous souhaitez que je documente certains points auxquels j'ai fait référence pendant mon intervention.

Pour conclure, je pense qu'il est extrêmement important de ne pas réduire la question de la souveraineté à l'hébergement, mais d'y inclure également la question de l'usage. De cette manière, nous ne nous retrouverons pas dans cinq ans à tenir les mêmes échanges, cette fois sur l'intelligence artificielle. Les acteurs américains développent des services « managés » d'intelligence artificielle de façon très rapide. Cela est un sujet majeur : nous avons tous les atouts en France pour développer ces usages, mais nous risquons de nous retrouver dans quelques années dans la même situation qu'actuellement pour le *cloud*.

M. Philippe Latombe, rapporteur. Cela est tout à fait intégré. Je vous remercie.

Audition, ouverte à la presse, de Mme Laurence Jay-Passot, déléguée générale du groupement de coopération sanitaire des hôpitaux universitaires Grand Ouest (HUGO), et du professeur Marc Cuggia, professeur des universités-praticien hospitalier au centre hospitalier universitaire (CHU) de Rennes, sur la plateforme de données hospitalières Ouest Data Hub
(18 février 2021)

La séance est ouverte à 12 heures.

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos auditions consacrées à la thématique des données de santé et de la souveraineté numérique. Le Ouest Data Hub est une plateforme de données hospitalières permettant de regrouper de façon anonymisée les données de six établissements membres du groupement, à savoir les centres hospitaliers universitaires (CHU) d'Angers, de Brest, de Nantes, de Rennes, de Tours ainsi que l'institut de cancérologie du Grand Ouest.

Ce hub est un nouveau concentré des problématiques qui intéressent notre mission d'information. Il interroge notre capacité à procéder à des choix opérationnels qui garantissent à la fois la protection des données de nos concitoyens et un niveau le plus élevé possible de performance. Il s'agit de numériser rapidement notre système de santé pour gagner en maturité sur certaines technologies clés pour l'avenir et de rendre un service d'une qualité toujours croissante à nos concitoyens. Nous avons également – et l'actualité de ces derniers jours nous le rappelle à nouveau – le devoir d'assurer la plus haute sécurité possible de nos systèmes d'information contre les cyberattaques. Nous nous réjouissons donc d'échanger avec vous sur ces différents sujets.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

J'aimerais d'abord que vous nous présentiez en détail le Ouest Data Hub : son organisation, son fonctionnement et son actualité pour l'année 2021. Il me semble important de comprendre comment fonctionne cette plateforme de données de santé, dont l'objectif est de soutenir la recherche et l'innovation en santé.

Je souhaiterais également savoir comment l'action du Ouest Data Hub s'articule avec les autres hubs de données de santé, et en particulier au niveau national avec le Health Data Hub, dont nous avons auditionné la directrice plus tôt ce matin. Il s'agit pour nous de comprendre comment le Ouest Data Hub s'intègre à l'écosystème du numérique en santé.

Le second sujet que je souhaite aborder avec vous a trait au cœur des travaux de notre mission d'information : la souveraineté numérique dans le domaine de la santé. Comment percevez-vous cet enjeu et comment l'avez-vous intégré à vos choix opérationnels au sein du Ouest Data Hub ? Quels ont été les choix techniques réalisés pour l'hébergement des données de santé et leurs motivations ? Cela nous permettra également d'échanger sur l'existence, ou non, d'arbitrages entre performance et sécurité à court et à moyen termes.

Enfin, et M. le président l'a souligné, l'actualité récente est marquée par des cyberattaques contre les systèmes d'information des établissements de santé. Face à la

sophistication de la menace cyber, comment est-il possible, selon vous, de garantir un niveau de protection maximale à nos infrastructures numériques, en particulier dans le domaine de la santé ?

Mme Laurence Jay-Passot, déléguée générale du groupement de coopération sanitaire des hôpitaux universitaires Grand Ouest (HUGO). Le Ouest Data Hub est un hub interrégional de données de santé qui permet de mener des études nécessitant d'agréger des données issues des entrepôts de données de santé des six établissements que vous avez mentionnés. Sa création s'inscrit dans une stratégie volontariste sur les données massives en santé qui a été construite, depuis plusieurs années, par notre réseau de CHU. Cette stratégie poursuit trois objectifs principaux. Le premier est de potentialiser l'expertise de nos CHU en matière de données, en s'appuyant à la fois sur le réseau des experts en données et sur les réseaux d'experts cliniciens du Grand Ouest. Le deuxième objectif est de pouvoir atteindre, par un travail collectif, une masse critique nécessaire pour réaliser des projets d'envergure. Enfin, le troisième objectif est de nous interfacer avec l'écosystème en santé et numérique sur notre territoire afin de favoriser et de servir l'innovation.

La caractéristique principale de ce hub interrégional est qu'il s'inscrit dans une logique de maîtrise de toute la chaîne de la donnée – depuis la production de la donnée, la structuration de sa collecte puis sa mise en qualité et jusqu'à son usage. Ainsi nous avons toujours le souci de rester en lien avec les professionnels de terrain et les cliniciens.

Il est tout d'abord important d'expliquer pourquoi notre CHU a fait le choix d'exploiter de façon prioritaire les données massives en santé.

Pr Marc Cuggia, professeur des universités, praticien hospitalier au centre hospitalier universitaire (CHU) de Rennes. L'informatisation des données de santé crée un potentiel de transformation et d'innovation : nous pouvons utiliser ces données de santé pour engendrer de l'information et de nouvelles connaissances grâce à des méthodes en plein développement, comme les fouilles de données et l'intelligence artificielle.

Les cliniciens et les acteurs de l'écosystème identifient plusieurs champs d'usages de ces données. Tout d'abord, ces données sont utiles pour soutenir la recherche biomédicale. Elles peuvent servir, par exemple, à identifier de nouveaux traitements ou de nouveaux biomarqueurs, à soutenir la recherche clinique par la réalisation d'études de faisabilité ou encore d'études populationnelles dans le champ de l'épidémiologie.

Ces données servent également la prise de décision, puisqu'elles fournissent des outils d'aides à la prescription ou à l'interprétation des examens biologiques. Elles permettent ainsi de mettre au point des outils qui vont aider le clinicien dans la prise en charge des patients.

Ces données alimentent également le champ de la vigilance et de la veille sanitaire. Au-delà de la veille sanitaire lors des épisodes épidémiques, les données permettent d'évaluer les traitements en vie réelle et de documenter leurs effets indésirables. Elles contribuent également à la matériovigilance, c'est-à-dire à la surveillance des dispositifs médicaux en vie réelle. L'usage de données massives en vie réelle est une source d'information extrêmement riche.

Enfin, les données contribuent au pilotage du système de santé. L'accès à des données transversales permet de mieux appréhender les parcours de santé de nos concitoyens et d'adapter le système en fonction des contraintes. Tous ces domaines sont extrêmement importants et peuvent bénéficier des données massives.

Mme Laurence Jay-Passot. Partant de ce constat partagé, nous avons identifié un enjeu stratégique à exploiter ces gisements de données. Nous nous sommes ainsi engagés dans une démarche en plusieurs étapes – toutes sont fondatrices du hub interrégional aujourd'hui en place.

La première étape fondamentale a consisté à structurer les gisements de données dans chaque établissement. Nous avons fait en sorte que les CHU puissent chacun développer un entrepôt de données de santé de la manière la plus convergente et homogène possible. Cela nous permet aujourd'hui de disposer de six entrepôts de données qui fonctionnent en utilisant des technologies similaires.

La seconde étape, débutée il y a plusieurs années, a consisté à mutualiser dès l'origine les expertises sur les données massives en santé et à mettre en réseau ces entrepôts de données de santé. Grâce à cette base, nous avons créé, il y a deux ans, un data hub partagé et sécurisé, le Ouest Data Hub, en même temps que nous travaillions à la stimulation des usages et à l'exploitation multicentrique des données, pour pouvoir d'emblée tester la plateforme interrégionale sur de vrais projets.

Ce hub interrégional n'a de sens que s'il s'appuie sur des centres de données cliniques solides : les entrepôts de données des établissements qui composent notre réseau constituent le socle fondamental du hub. Ces centres de données ont été construits en plusieurs années dans notre interrégion. Chaque CHU du réseau propose ainsi, dans son centre de données clinique, une expertise pluridisciplinaire, un accompagnement auprès des professionnels de santé et des éléments d'infrastructure normalisés qui garantissent la sécurité des données. Ces centres de données cliniques sont le fondement de notre Ouest Data Hub.

Ces centres de données cliniques prennent appui sur un réseau d'expertises structuré. Ceci permet de disposer d'une vraie feuille de route technique et opérationnelle pour travailler ensemble et d'évoluer vers une exploitation multicentrique des données.

La plateforme interrégionale de données de santé Ouest Data Hub rassemble six hôpitaux et est permise par le déploiement d'une technologie commune dans les différents centres de données cliniques des établissements. La plateforme donne ainsi accès à un volume très important de données issues des six établissements. Le catalogue est nourri par les informations produites par les patients et continue à s'enrichir régulièrement. Ce potentiel considérable de données a du sens car ces données sont homogènes et de qualité : la possibilité d'exploiter les données de manière intéressante est un enjeu capital.

La plateforme interrégionale est composée de plusieurs éléments. La dimension infrastructure est essentielle pour connecter et faire communiquer entre eux les différents centres de données cliniques. L'infrastructure est hébergée au sein du CHU de Nantes. Le Pr Marc Cuggia détaillera plus tard ses éléments de logiciels très spécifiques.

Nous avons ensuite mis en place une gouvernance afin de définir les règles de partage et d'accès aux données et de rappeler le cadre éthique, déontologique et juridique qui doit être appliqué. La particularité de notre Ouest Data Hub est de mobiliser des structures juridiques distinctes, car chaque CHU constitue une personne morale propre.

Enfin, une politique scientifique qui s'articule autour des usages possibles des bases de données est animée grâce au réseau d'experts et à une politique d'appels à projets.

La gouvernance du Ouest Data Hub est structurée à plusieurs niveaux. Le pilotage stratégique est organisé par un comité stratégique impliquant les gouvernances des six établissements. Le pilotage scientifique, incarnée par une direction scientifique tripartite, permet d'orienter les choix que nous faisons. Nous avons également organisé un pilotage opérationnel sous la forme d'un guichet unique, qui permet de répondre aux sollicitations et de faire vivre cette plateforme. Nous avons enfin été attentifs à la dimension éthique et juridique de notre dispositif, c'est pourquoi nous avons mis en place un comité scientifique et éthique dédié. Un délégué à la protection des données (DPO) a également été choisi.

L'année 2019 et le premier semestre de l'année 2020 ont été consacrés à la conception et à la structuration de cette plateforme interrégionale ainsi qu'à la constitution du socle de données commun qui permet de la nourrir. Depuis la mise à disposition technique de notre plateforme à l'été 2020, nous sommes passés dans une phase de projet. Il s'agit maintenant de mener à bien les premiers projets interrégionaux utilisant cet outil, de poursuivre l'enrichissement des catalogues de données et de réfléchir au modèle économique de cette plateforme, qui est également un sujet important.

M. Philippe Latombe, rapporteur. Comment avez-vous construit l'architecture des différents entrepôts de données ? Quelles technologies utilisez-vous ?

Pr Marc Cuggia. Nous utilisons une technologie développée au sein du laboratoire de l'Institut national de la santé et de la recherche médicale (Inserm) dans lequel je travaille, en lien avec le CHU de Rennes. Il s'agit de technologies assez standard dans le domaine des données massives et du développement logiciel. L'objectif est d'intégrer les données du système d'information hospitalier dans les entrepôts locaux. Cette technologie est le fruit d'une activité de recherche et développement menée depuis plusieurs années. Un élément clé du déploiement était de s'adosser à une logique industrielle pour pouvoir déployer, alimenter et construire ces entrepôts. Pour cela, nous avons noué un partenariat avec la société Enovacom, aujourd'hui devenue une filiale d'Orange. Nous avons couplé cette technologie avec le savoir-faire de cette société pour nous aider à construire ces flux de données. Cela nous a permis à nous, laboratoire de recherche et CHU de Rennes, de nous focaliser sur l'innovation sur ces sujets et d'assurer un déploiement et une maintenance industriels de ces socles de données au niveau de chaque établissement.

Le développement de la plateforme Ouest Data Hub, c'est-à-dire de la plateforme collectant les données, a également été réalisé par notre équipe à Rennes. Nous avons développé l'ensemble des éléments logiciels et de mise en œuvre de cette plateforme. La partie technologique ayant trait à la sécurité et aux serveurs est assurée par le CHU de Nantes, qui met à disposition une infrastructure de stockage et de calcul. Nous nous appuyons pour cela sur son savoir-faire en matière d'hébergement de données de santé. Le CHU de Nantes est en effet l'un des établissements hébergeurs de données de santé disposant de la plus grande expérience dans ce domaine. Ce dispositif a donc été élaboré dans une logique de coconstruction grâce à des dynamiques de recherche et développement à la fois académiques et industrielles.

Nous utilisons des technologies à l'état de l'art. Pour réaliser des traitements sur des données complexes, il faut bénéficier de capacités de calcul mais aussi de logiques industrielles pour que ces outils puissent être déployés et maintenus par les directions des systèmes d'information (DSI). Les entrepôts sont hébergés directement par les DSI de chaque établissement. Le Ouest Data Hub, quant à lui, est hébergé par le CHU de Nantes car cet établissement est hébergeur de données de santé. L'écosystème s'est construit de cette manière.

M. Philippe Latombe, rapporteur. Les données de santé sont-elles pseudonymisées et sécurisées ?

Pr Marc Cuggia. Nous avons deux niveaux d'agrégation. Le premier niveau est celui de l'établissement : un entrepôt de données est géré par le centre de données cliniques de chaque établissement. Nous récupérons les données produites par les différents logiciels métiers de l'établissement et nous alimentons ainsi l'entrepôt de données avec des données dé-identifiées afin qu'elles puissent être utilisées à des fins d'innovation et de recherche. Chaque établissement reste souverain dans l'usage de ses données. Les établissements traitent donc en premier lieu les données et peuvent les mettre à disposition de leurs collègues cliniciens pour des projets monocentriques, par exemple.

Dès lors que nous devons partager des données entre plusieurs établissements, nous nous appuyons sur la plateforme Ouest Data Hub qui permet de collecter les données sur projet. Ces données, collectées à partir des différents entrepôts de données, sont dé-identifiées puis collectées et agrégées sur projet. Nous ne déversons pas l'ensemble des données sur le Ouest Data Hub : nous mettons au catalogue ces données, puis nous ne mettrons à disposition que les données nécessaires à la réalisation d'une étude. Ces données sont agrégées dans des espaces projets dédiés à chaque projet, sécurisés et cloisonnés. En quelque sorte, les données quittent la bulle sécurisée de l'entrepôt de données de chaque établissement pour rejoindre une autre bulle sécurisée dans laquelle se réalisent les traitements.

M. Philippe Latombe, rapporteur. Sous quelle forme se présentent ces entrepôts de données dans chaque établissement ? La bulle de l'espace projet est-elle hébergée en *cloud* ou bien dans le serveur physique de l'endroit où se déroule la recherche ?

Pr Marc Cuggia. Les données sont hébergées sur des serveurs au sein de chaque établissement. Les données sont donc physiquement présentes dans des serveurs hébergés dans chaque CHU, sous la responsabilité des DSI. Les centres de données cliniques sont là pour exploiter les données pour l'établissement. La plateforme Ouest Data Hub est également hébergée au sein du CHU de Nantes, sous la direction de la DSI qui met à disposition les serveurs sécurisés et les ressources de stockage et de calcul pour réaliser les travaux. L'accès aux données présentes sur le Ouest Data Hub est strictement réservé aux équipes projets qui vont exploiter les données mises à disposition dans leur espace projet. Cet écosystème est complètement intégré. La plateforme Ouest Data Hub est en capacité de collecter les données issues de chaque établissement en fonction des besoins de chaque projet.

M. Philippe Latombe, rapporteur. Vous avez donc opté pour un hébergement physique. Vous n'utilisez pas de *cloud*.

Pr Marc Cuggia. Nous n'utilisons pas du tout de *cloud*.

M. Philippe Latombe, rapporteur. Comment allez-vous procéder avec le Health Data Hub, qui, lui, utilise des solutions de *cloud* ?

Pr Marc Cuggia. Nous conduisons actuellement un projet avec le Health Data Hub. Nous agrégeons un certain nombre de données collectées à partir des centres de données cliniques. Ces données sont dé-identifiées et transmises dans l'espace projet mis à disposition par le Health Data Hub. Les données collectées dans le cadre du projet seront couplées avec les données de l'Assurance maladie. Ainsi, des jeux de données seront extraits de chaque entrepôt de données correspondant aux besoins de l'étude, puis déposés sur la plateforme du Health Data Hub. L'Assurance maladie extraira elle aussi un jeu de données, qu'elle déposera

sur la plateforme. Nous réaliserons alors l'appariement de ces données pour les besoins de l'étude. La logique est la même : les données quittent une bulle sécurisée pour rejoindre une autre bulle sécurisée. Les données collectées ne sont pas anonymisées mais dé-identifiées : l'on applique des algorithmes qui vont supprimer les éléments de ré-identification potentielle des données.

M. Philippe Latombe, rapporteur. Nous venons de conduire une audition avec le Health Data Hub. L'utilisation du *cloud* et le recours à des solutions américaines, notamment Azure de Microsoft, ont donné lieu à beaucoup de discussions. Comprenez-vous le choix fait par le Health Data Hub ? Le Health Data Hub aurait-il pu opter pour la même solution physique que vous et la développer à une échelle beaucoup plus importante ?

Pr Marc Cuggia. J'ai été l'un des trois copilotes de la mission de préfiguration du Health Data Hub. La mission de préfiguration visait à mettre à disposition un ensemble de solutions techniques pour permettre le traitement des données de façon sécurisée et pour garantir une souveraineté nationale ou européenne sur ces sujets. La lettre de mission confiée par Mme la ministre mentionnait clairement ces éléments.

Les solutions, qu'elles soient complètement *indoor* ou *cloud*, peuvent être utilisées. Je n'ai pas réellement compris pourquoi l'on a fait le choix d'utiliser des technologies qui ne sont pas portées par des acteurs français ou européens, si l'on souhaitait mettre en place une solution souveraine. Cela est paradoxal.

Nous avions exploré un certain nombre de pistes lors de la mission de préfiguration. La structure TeraLab est une initiative très intéressante, qui a été développée pour mettre en place des traitements *big data* pour accompagner différents projets. Elle aurait pu constituer une bonne solution, au moins transitoire, pour tester et organiser le déploiement et l'usage du Health Data Hub.

Ceci étant dit, les choix opérés étaient sans doute justifiés d'un point de vue technologique. L'architecture Azure est très performante sur le plan du traitement des données. Mais il est vrai que je n'ai pas très bien compris pourquoi nous n'avons pas pu examiner d'autres solutions.

Un certain nombre d'éléments de discussion ont été apportés à la suite du *Cloud Act*. Les acteurs américains hébergent aussi des données de santé : Microsoft est homologué hébergeur de données de santé. Dans ce cas, ces données sont nominatives et orientées sur le soin.

Des solutions viables, *indoor* ou sous *cloud*, existaient et elles auraient pu être explorées, au moins le temps d'une phase projet et de montée en charge. Il y a également une volonté de réversibilité de ces choix, c'est-à-dire une volonté d'utiliser un environnement plus souverain. À partir du moment où les données sont sécurisées, nous n'avons pas de raison de ne pas contribuer à cet effort national par le projet HUGO-Share, car le Health Data Hub est un formidable projet.

Les auditions conduites dans le cadre de la mission de préfiguration nous ont montré que l'écosystème était très enthousiaste à l'idée de mettre en place un projet qui l'aide à développer des innovations. Il faut désormais probablement réfléchir à la façon d'y arriver, repenser ces choix et coconstruire. La mission de préfiguration avait insisté sur le fait que l'ensemble des acteurs devait être impliqués dans la coconstruction de ce hub national. Le Ouest Data Hub a appliqué cette stratégie pour se structurer et s'organiser : le hub doit être au

service de l'écosystème. Il convient donc d'orienter la feuille de route du Health Data Hub pour nous aider à développer ces logiques territoriales.

M. Philippe Latombe, rapporteur. Votre architecture est-elle justifiée par votre organisation en réseau de CHU ? Le poids de l'histoire a-t-il joué dans cette architecture ? Le Health Data Hub, au contraire, est une création ex-nihilo – cela pourrait expliquer le fait que d'autres choix technologiques ont été opérés.

Pr Marc Cuggia. Si l'histoire de l'informatisation de l'hôpital est ancienne, l'informatisation du dossier médical est, en revanche, relativement récente. Dès lors que nous numérisions les données du dossier médical, nous avons souhaité les utiliser à des fins de recherche et d'innovation.

Au départ, un prototype qui nous permettait de croiser ces données en format papier avait été développé. La vague de la santé numérique a complètement transformé le secteur : nous avons désormais à notre disposition des capacités de stockage et des méthodes qui nous permettent de répondre à des questions médicales.

Un prototype avait donc été développé par mon équipe à Rennes. À Brest, une équipe avait, elle, déjà pensé la création d'un centre de données cliniques. Nous avons développé un projet commun et nous avons déployé ces centres de données cliniques. Nous étions, dès le départ, convaincus que nous devions le faire de manière groupée. Nous ne pouvions pas dégager d'axes d'innovation isolément. La création des centres de données cliniques nous a donc amenés à nous interroger sur des projets multicentriques et des moyens communs. La plateforme actuelle est ainsi le fruit d'un travail de coopération existant depuis très longtemps.

Nous sommes confrontés à des problématiques très complexes de qualité de données. En France, notre système de données de santé est extrêmement fractionné ; aucun système d'information ne ressemble à un autre. L'enjeu de collecter les données et de les harmoniser est essentiel, et implique tout un panel d'acteurs. Cela implique des actions tout au long de la chaîne de production de données et d'expertise. C'est tout l'enjeu des centres de données cliniques.

Mme Laurence Jay-Passot. Il existe une dimension historique aux choix opérés. Mais au-delà de cela, nous avons conduit des choix stratégiques parfaitement assumés. En premier lieu, nous avons fait le choix d'un dispositif qui nous permet de maîtriser la donnée de bout en bout, pour des raisons d'éthique et d'acceptation par les patients et les communautés médicales. Nous avons également fait le choix de garder un lien très fort avec le terrain, les investigateurs et les cliniciens. Ce lien garantit que les données seront de qualité, aussi bien dans leur collecte que dans leur traitement.

Les choix techniques et d'organisation sont donc assis sur ces convictions. Nous appliquons ainsi un principe de subsidiarité : les centres font localement tout ce qui leur est possible de faire. Tous les projets n'ont pas vocation à être portés à l'échelon interrégional. Mais dès lors que nous identifions un intérêt à massifier, nous utilisons l'infrastructure commune.

Nous avons discuté de la création d'un entrepôt mutualisé. Nous avons jugé qu'un entrepôt mutualisé n'apporterait pas de plus-value particulière pour le moment et dans le contexte actuel. Ce dispositif est en effet extrêmement complexe et pourrait poser des questions de sécurisation. Nous avons conclu que nous pouvions travailler très efficacement et répondre à nos objectifs avec le modèle des plateformes locales.

M. Philippe Latombe, rapporteur. Cela a-t-il nécessité de mener un important travail de pédagogie en direction des équipes ? Avez-vous eu besoin d'acculturer les équipes à la nécessité de partager les données ? Votre gouvernance, avec un comité d'éthique et un DPO spécialisé, a-t-elle permis lever les freins et les réticences qui pouvaient exister ?

Pr Marc Cuggia. La création de la confiance est un sujet extrêmement important. Les centres de données cliniques sont créés pour exploiter les données produites par les différents services des hôpitaux de manière transversale. Cette chaîne de confiance est donc fondamentale.

La pédagogie se met en place très rapidement car la plateforme que nous avons développée répond à des questions posées par les cliniciens. Des réponses qu'il n'était pas possible d'obtenir auparavant s'obtiennent maintenant de manière plus fluide et plus facile. Il s'agit d'une pédagogie par l'exemple. Cela crée une boucle vertueuse, car la prise de conscience de ces résultats a un impact sur la qualité des données ; et cela crée un effet d'entraînement.

Les centres de données cliniques accueillent également en leur sein des cliniciens qui se forment au code, aux méthodes et aux technologies d'intelligence artificielle. Cela permet à nos collègues cliniciens de développer de nouvelles compétences et de s'approprier ces outils.

Le comité scientifique et éthique interrégional est un élément majeur de notre gouvernance. Il doit répondre aux problématiques de qualité scientifique des projets, d'intérêt de santé publique et de protection des données. Ce comité réunit les établissements membres d'HUGO ainsi qu'une association de patients et des éthiciens. Il porte donc un regard véritablement pluridisciplinaire sur ces enjeux.

Mme Laurence Jay-Passot. La pédagogie est un sujet permanent. Une maturité collective se développe dans le Grand Ouest depuis plusieurs années. Nous avons constaté une prise de conscience de l'intérêt du travail collaboratif, de l'intérêt de mutualiser les données et de mener des projets multicentriques au travers de nos réseaux thématiques. Les groupes de travail thématiques sont aujourd'hui tout à fait matures pour développer les usages des données massives en santé.

Nous associons toujours à la dimension d'infrastructure un autre volet : celui de la stimulation des usages et de l'animation de l'écosystème de la recherche et de l'innovation. En parallèle de la construction du dispositif, nous avons ainsi lancé un appel à projets pour démontrer d'emblée l'intérêt de la plateforme.

M. Philippe Latombe, rapporteur. Les patients sont-ils au courant de l'existence d'HUGO, de l'utilisation des données et de la protection qu'ils peuvent en attendre ? Dans le cas du Health Data Hub, le grand public s'est également posé de nombreuses questions sur l'utilisation des données de santé.

Mme Laurence Jay-Passot. Nous avons communiqué régulièrement sur le sujet en nous appuyant sur nos centres de données cliniques. Je n'ai pas le sentiment que les discussions sur le Health Data Hub aient rejailli particulièrement sur le déroulement de nos projets. Cela s'explique en partie par le fait que notre Ouest Data Hub ne naît pas de rien : il est l'aboutissement de la constitution des centres de données cliniques, au sujet desquels des communications régulières ont été faites auprès du grand public et qui respectent toutes les

exigences de la Commission nationale de l'informatique et des libertés (CNIL) quant à la formation des entrepôts et à l'information des patients.

M. Philippe Latombe, rapporteur. Quelle est votre sensibilité aux cyberattaques, et plus généralement à la sécurité et à l'atteinte à l'intégrité des données ? Votre architecture fragilise-t-elle la sécurisation, ou au contraire, constitue-t-elle un avantage en la matière ?

Pr Marc Cuggia. Un certain nombre de mesures technologiques et organisationnelles sont nécessaires pour renforcer la sécurité. S'agissant des cyberattaques, il faut éviter les effets d'attractivité ou « pot de miel ». C'est une des raisons qui nous a conduit à ne partager des données que sur projets : ne sont donc mises à disposition sur la plateforme hébergée à Nantes que les données strictement liées à des projets.

Nos établissements entrent dans une logique de sécurisation. Le CHU de Nantes est hébergeur de données de santé, et le CHU de Rennes est en cours d'obtention de la labellisation. Les mesures de sécurité en sont donc considérablement augmentées. Nous sommes hébergés au sein du système d'information de l'hôpital. L'entrepôt de données collecte donc des données, qui sont stockées au sein de l'hôpital ; ces données sont par ailleurs toutes déjà présentes dans les différents outils utilisés par les médecins. Nous nous appuyons sur le savoir-faire de la DSI pour assurer la sécurité des données.

Les données sont pseudonymisées. Nous avons nourri des échanges très poussés avec les équipes techniques de la CNIL, qui nous ont beaucoup aidés. Ils nous ont exprimé un certain nombre de préconisations que nous avons mises en œuvre. Nous veillons à ce que les mesures de sécurité maximales puissent s'appliquer.

La cybersécurité est évidemment un sujet de recherche et développement. Dans le cadre du développement de la plateforme, nous menons des projets de recherche et innovation sur des solutions comme le crypto-tatouage de bases de données ou l'avatar des données. Nous souhaitons expérimenter ces solutions dans nos environnements. Les données massives en santé constituent un objet d'innovation en cybersécurité. Nous sommes sensibles au fait que les données confiées par les patients soient tout à la fois protégées et permettent l'innovation et la recherche, au bénéfice du patient.

M. Philippe Latombe, rapporteur. Développez-vous ces solutions en interne ou faites-vous appel à des solutions développées par des sociétés privées extérieures ?

Pr Marc Cuggia. Je vous présenterai le projet actuellement mené sur le crypto-tatouage des bases de données. Cette technologie a été développée dans un laboratoire cyber universitaire et nous allons l'expérimenter dans le centre de données cliniques du CHU de Rennes, puis nous en évaluerons les performances. Cette technologie doit permettre d'assurer la traçabilité des traitements sur des données par tatouage des données.

L'enjeu est de créer un terrain multidisciplinaire pour appliquer ces objets de recherche dans nos domaines. Nous souhaitons, si les technologies que nous expérimentons sont suffisamment éprouvées et matures, qu'elles puissent être développées avec des start-up et qu'elles deviennent un objet industriel. Nous avons donc vocation à travailler avec des start-up et des industriels sur nos sujets. Nous travaillons également en partenariat avec des start-up pour le développement d'outils d'aide au diagnostic.

M. Philippe Latombe, rapporteur. Ce projet a nécessité une homogénéisation des données et des systèmes d'information. Cela a-t-il un effet d'entraînement sur d'autres domaines, pas nécessairement ceux de l'informatique et de la recherche ?

Mme Laurence Jay-Passot. Oui, cela a plusieurs effets d'entraînement. Nous cherchons à inventer un modèle de hub interrégional ; notre action a du sens si elle peut permettre la structuration d'autres hubs interrégionaux sur le territoire. Nous travaillons très étroitement avec deux autres réseaux de CHU constitués plus récemment qu'HUGO : le G4 dans le Nord et le groupement Grand Est. Ils suivent la même trajectoire de constitution d'un hub interrégional. Cela fait sens de disposer de hubs interrégionaux qui pourraient s'articuler avec le dispositif national, comme cela avait été imaginé dans le rapport de préfiguration.

Il existe également des sujets connexes pour lesquels un effet d'entraînement se fait sentir et permet d'avancer plus loin les dynamiques de partage de données et d'expertises. C'est le cas, par exemple, dans le Grand Ouest de la réflexion sur la génomique. Cette dynamique de partage est permise par la grande transversalité des données massives en santé.

Pr Marc Cuggia. Nous avons largement partagé notre expérience avec les autres établissements en matière de structuration des entrepôts de données, de qualité, de protection, de gouvernance, d'usages. Cela crée un effet d'entraînement national très important, qui se traduit par la mise en place d'entrepôts de données dans la plupart des CHU de France et dans les centres de lutte contre le cancer, ainsi que par la création d'équipes spécialisées dans ces domaines.

Je souhaite saluer l'initiative InterHop qui intervient sur des sujets très techniques. Il est nécessaire que l'on s'accorde sur des standards et des terminologies pour harmoniser nos données. J'insiste sur le fait que l'harmonisation n'est pas encore complète dans le Grand Ouest. Ce processus est progressif et nos efforts sont constants en la matière.

Je salue également les initiatives comme celle portant le modèle Osiris, qui normalise les données dans le champ de la cancérologie pour la réutilisation secondaire des données. Ces initiatives sont portées par des équipes d'informatique médicale et il faut absolument les encourager. Le Grand Ouest va développer ses propres projets, certes, mais l'enjeu est national, voire international. Ces travaux ne sont pas forcément très visibles pour le grand public mais ils sont extrêmement importants.

L'effet d'entraînement est également majeur pour les éditeurs de logiciels médicaux, qui développent des outils utilisés par les cliniciens. Il existe un enjeu majeur en matière de structuration et de normalisation des données ainsi que d'utilisation de standards dans nos systèmes d'information. L'Agence du numérique en santé a publié une stratégie en la matière. L'innovation et la recherche vont bénéficier directement de ces efforts au long cours. Il est essentiel que les industriels mettent en œuvre les préconisations de standardisation, afin que les équipes des établissements de santé puissent facilement disposer des données.

L'enjeu de la qualité et de la maîtrise de la donnée est crucial tout au long de la chaîne de traitement de la donnée, depuis le lit du patient jusqu'à l'innovation. Une stratégie forte doit certainement être mise en place à ce sujet aux niveaux national et européen. L'Allemagne, par exemple, l'a fait.

Mme Laurence Jay-Passot. Nous souhaiterions que cet effet d'entraînement alimente également la réflexion sur le modèle économique des entrepôts de données et des hubs interrégionaux. Ce travail, que le Pr Marc Cuggia a très bien décrit, nécessite un fort

investissement aussi bien en matière d'infrastructures que de ressources humaines. La région Grand Ouest a mené une action volontariste en la matière : elle a fait le choix d'aligner une énergie collective avec des choix financiers collectifs. Mais une réflexion doit s'engager sur son modèle économique qui, aujourd'hui, n'est pas du tout accompagné. Nous sommes convaincus que les hubs interrégionaux ont toute leur place pour collecter des données et les mettre en qualité, puis les articuler avec un dispositif national. Mais il va falloir nous aider collectivement à le faire. Je comprendrais aisément que toutes les interrégions et tous les groupements d'établissements ne fassent pas les mêmes choix que ceux que nous avons faits.

M. Philippe Latombe, rapporteur. Faut-il penser un modèle économique pour les hubs interrégionaux ? Faut-il que vous puissiez vendre les données ? Comment ces sources de revenus pourraient-elles être compatibles avec tous les efforts déployés en faveur de l'éthique et de la protection des données ?

Mme Laurence Jay-Passot. Ce modèle économique est encore à inventer, mais il est nécessairement mixte. La structuration des entrepôts de données et des centres de données cliniques n'est aujourd'hui pas intégrée dans le financement des hôpitaux. Cela soulève un sujet de financement.

Il pourrait également y avoir un sujet de structuration des hubs interrégionaux. La possibilité avait été évoquée de lancer des appels d'offres structurants pour les hubs interrégionaux.

La valorisation des données des entrepôts locaux et des plateformes interrégionales constitue un autre sujet. Nous ne pouvons pas vendre les données en tant que telles, mais nous pouvons valoriser par un échange monétaire le travail fourni par nos équipes en termes de mise en qualité des données et de réponse à une question scientifique. Dans un conventionnement, nous pouvons mettre en avant l'expertise que nos équipes sont capables d'apporter en mobilisant des données pour répondre à une question posée. Cela pourrait participer de la constitution d'un futur modèle économique, mais il existe encore peu de choses sur le sujet.

M. Philippe Latombe, rapporteur. Avez-vous chiffré le coût en investissements de la création d'HUGO ? Si un groupement devait aujourd'hui créer un tel dispositif en partant de zéro, combien cela lui coûterait-il ? De tels investissements constituent un choix pour l'avenir. Je m'interroge sur les fonds qui devraient être mobilisés pour créer ces dispositifs régionaux, par exemple dans le plan de relance actuel.

La création d'HUGO a-t-elle apporté un plus à l'écosystème de la recherche publique ou privée dans l'Ouest ? A-t-elle drainé, par exemple, l'installation d'entreprises ou de structures de biotechnologies ?

Mme Laurence Jay-Passot. Avant toute chose, une clarification terminologique : HUGO est notre réseau de CHU. L'Ouest Data Hub est l'un des projets qu'il porte en matière de données massives. Nous portons par ailleurs beaucoup de projets en soin, enseignement et recherche.

Le coût d'amorçage de la plateforme comprend un coût d'hébergement et un coût de ressources humaines. Ce coût est aujourd'hui de l'ordre de 300 000 euros par an, couvrant uniquement la partie mutualisée. En revanche, si l'on chiffre la contribution apportée par les centres données cliniques à chacun des projets, les coûts sont évidemment plus élevés : je les évalue entre 500 000 euros et un million d'euros à moyen terme.

Il n'est pas possible de créer une plateforme interrégionale sans disposer de centres de données cliniques et d'entrepôts de données de santé dans les établissements. Cela représente un vrai coût. Aucun centre de données cliniques n'est le même et ne requiert le même investissement en infrastructure et en ressources humaines. Néanmoins, nous savons qu'*a minima*, en conditions de fonctionnement pérennes, un établissement doit investir près de 400 000 euros chaque année pour faire fonctionner son centre de données cliniques déjà existant. Ce coût ne comprend pas la constitution initiale du centre de données. Ces sommes, mises bout à bout, pèsent sur les budgets. Ces évaluations sont, qui plus est, très minimalistes. Si l'on voulait inclure le temps investi pour faire grandir ce genre de projet, cela nécessiterait de chiffrer encore davantage de charges indirectes que je n'ai pas citées.

Pr Marc Cuggia. Je répondrai à votre question, s'agissant de la valorisation de la recherche. L'exploitation des données massives dans le champ de la santé est un sujet de compétition internationale. Nos centres sont encore beaucoup trop peu dotés, en termes de matériels et de chercheurs, pour pouvoir s'intégrer dans cette compétition, qui se développera de manière très forte dans les prochaines années. Des centres aux États-Unis sont, par exemple, composés de 75 enseignants-chercheurs permanents. L'Allemagne a fait le choix de mailler l'ensemble de son territoire avec des centres de données : leur stratégie a été de doter les établissements de *data information centers*. 120 millions d'euros ont donc été investis sur tout le territoire pour constituer des centres de données cliniques, créer des postes de permanents hospitalo-universitaires, embaucher des *data scientists*. Je pense que l'infrastructure ne fera pas l'innovation. L'enjeu principal réside dans le potentiel humain de formation et d'interdisciplinarité sur le terrain. C'est cela qui nous permettra d'avoir collectivement une chance de développer une souveraineté sur les enjeux de numérique en santé. L'écosystème des établissements publics à caractère scientifique et technologique (EPST), des start-up, des industriels est extrêmement important.

En termes d'attractivité, nous constatons de plus en plus de sollicitations d'acteurs qui souhaiteraient développer ou codévelopper avec nous des projets sur les données. Cela suppose de monter en charge et de construire notre capacité à accompagner ces acteurs. L'enjeu est pour nous très important de pouvoir répondre à cette dynamique. Nous essayons de mettre cela en œuvre avec le Ouest Data Hub, grâce à une gouvernance qui se veut transparente. Nous avons une volonté collective de réussir et d'innover. Mais il ne s'agit pas d'être dans une logique purement financière : en tant que chercheur, ce qui m'intéresse est que le contenu de nos recherches serve avant tout au patient. Cela est notre mission première. Nous ne nous interdisons pas de travailler avec des industriels, mais l'enjeu est de faire grossir ces centres de données cliniques et cette expertise sur le territoire.

Mme Laurence Jay-Passot. Effectivement. Sinon, nous serons très limités par rapport au potentiel que représentent ces données.

M. Philippe Latombe, rapporteur. Croyez-vous que ce fonctionnement en hub, qui fonctionne pour les données massives en santé, peut servir à d'autres secteurs ? Cela vaudrait-il la peine de le développer pour d'autres domaines que les données de santé ?

Mme Laurence Jay-Passot. Évidemment. Nous avons fait le choix de privilégier ces modes de fonctionnement en hub ou en plateforme, et nous considérons que dès que la notion de masse critique fait du sens, nous devons construire une réponse collective. Cela ne veut pas dire centraliser et perdre le lien avec les initiatives locales. Le modèle de hub est absolument reproductible dans d'autres domaines, si on le conçoit comme un dispositif qui permet de mutualiser uniquement ce qui doit l'être et que l'on arrive à penser des systèmes de gouvernance agiles, qui continuent à s'appuyer sur toutes les compétences disponibles dans

les centres locaux. Nous y croyons très fortement. Il existe plusieurs sujets – et les données massives en santé en sont un – pour lesquels le modèle de hub sera pertinent, s'il est dupliqué à l'échelle interrégionale sur l'ensemble du territoire.

Pr Marc Cuggia. Ces réflexions dépassent les données de santé *stricto sensu* et s'appliquent également à des projets mettant en œuvre des approches similaires, en lien avec les citoyens. Je citerai trois expériences auxquelles nous sommes associés. D'abord, Rennes Métropole travaille à mettre au point un portail des données personnelles qui vise à exploiter les données de transport, d'énergie, de santé à des fins de recherche et d'innovation. Une réflexion de hub pourrait être mise en place à ces fins. Ensuite, l'université de Sherbrooke au Québec a mis en place un projet similaire de système d'information apprenant ; le projet Pulsar de l'université de Laval, enfin, fait le lien entre les données de santé et les données de territoires. Des projets d'innovation très importants existent donc, qui ont un lien très fort avec les citoyens. Ces pistes me semblent extrêmement intéressantes à suivre pour pouvoir mettre en place une santé numérique durable.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous aborder un dernier sujet en matière de données de santé, que nous n'avons pas déjà évoqué au cours de l'audition ? À quoi devrons-nous être vigilants à l'avenir ?

Pr Marc Cuggia. Il faut garder à l'esprit que nos activités doivent être au service des patients. Les innovations que nous développons ont utilisé des données de qualité très variables, avec des méthodes de *machine learning* qui peuvent parfois poser des problèmes d'interprétabilité. Il y a donc un enjeu majeur d'évaluation des produits d'innovation, c'est-à-dire des algorithmes. Les algorithmes doivent être évalués au même titre qu'un dispositif médical ou qu'un produit de santé. Les équipes des CHU, de l'Inserm, tout le maillage de recherche clinique et d'innovation doivent se saisir de cette opportunité. Dans le Grand Ouest, nous avons mis en œuvre plusieurs tests de ces algorithmes en vie réelle, à la manière d'un essai clinique. Nous devons fermer la boucle : nous collectons des données de santé, nous en tirons des connaissances qui permettent de construire des outils utiles au patient et au clinicien, qui devront enfin être évalués. Ces algorithmes devront être évalués sur les patients suivant une véritable démarche de recherche clinique. Nous devons pouvoir mettre en place ce cercle vertueux. Cela suppose également d'entrer dans des logiques de normalisation et de labellisation des centres de données cliniques. Cela constitue un élément majeur de la confiance : il s'agit à la fois de la confiance du clinicien envers l'outil qu'il utilise tous les jours et de la confiance du patient.

Mme Laurence Jay-Passot. La réflexion du Pr Marc Cuggia a beaucoup de sens et remet toutes nos discussions en perspective.

M. Philippe Latombe, rapporteur. Je vous remercie.

Audition commune, ouverte à la presse, de M. Adrien Parrot, médecin-ingénieur, président, et de Me Juliette Alibert, avocate, membre de l'association InterHop
(18 février 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Bonjour à toutes et à tous. Je souhaite la bienvenue à Maître Juliette Alibert et à M. Adrien Parrot. Nous poursuivons avec vous des échanges très nourris, depuis ce matin, sur la thématique des données de santé et de la souveraineté numérique. InterHop est une association qui promeut et développe l'utilisation de logiciels libres et *open source* pour la santé – vous nous en direz plus tout à l'heure. Je crois savoir que vous prônez une utilisation autogérée des données de santé à l'échelle locale. Vous souhaitez en quelque sorte « dégoogliser » la santé numérique en proposant des hébergements de données décentralisés, transparents et éthiques. Vous œuvrez également en faveur du respect du Règlement général sur la protection des données (RGPD). Enfin, je dois noter que vous avez participé aux activités du comité SantéNathon à l'origine du recours intenté devant le Conseil d'État contre le choix effectué par « Health Data Hub » (HDH) en faveur du *cloud* de Microsoft pour l'hébergement de ces données. Nous sommes très heureux de pouvoir échanger avec vous aujourd'hui. La protection des données nous intéresse, évidemment, tout comme le recours à des logiciels libres et la question des communs numériques. Je vais laisser la parole à notre rapporteur afin qu'il introduise nos échanges.

M. Philippe Latombe, rapporteur. Je voudrais, en guise d'introduction, vous interroger sur trois points qui occupent nos travaux et qui ont été esquissés par M. le président. J'aimerais d'abord que vous nous présentiez votre association, InterHop, ainsi que votre combat en faveur des logiciels libres et de l'interopérabilité des systèmes d'information. Ces questions entrent en effet dans le champ des travaux de notre mission d'information. Ils suscitent un intérêt croissant et des discours parfois très tranchés. Nous sommes donc particulièrement intéressés par votre avis sur ces sujets que vous connaissez bien. Je résumerai ici mon propos au travers des questions suivantes : quel logiciel libre pourrait être utilisé ou substitué, selon vous, à des solutions propriétaires ? Quels seraient les avantages de cette approche ? Quels en sont également les limites et les risques ? Enfin, comment, selon vous, la question des communs numériques peut-elle nourrir aussi nos réflexions sur la souveraineté numérique ?

Le second point sur lequel je souhaiterais échanger avec vous concerne le HDH et l'hébergement des données de santé. InterHop, comme l'a rappelé M. le président, fait partie des membres du collectif SantéNathon, qui a attaqué en Conseil d'Etat le choix du HDH de recourir au *cloud* de Microsoft pour héberger les données de santé. Le ministre des Solidarités et de la Santé, M. Olivier Véran, s'est engagé à ce que le transfert du HDH vers un autre hébergeur que Microsoft intervienne dans un délai compris entre 12 et 18 mois. J'aimerais savoir quel regard vous portez sur la situation actuelle, quelle leçon il est possible, selon vous, d'en tirer pour les autres projets numériques portés par les pouvoirs publics. J'aimerais également vous entendre, dans le prolongement de cette réflexion, sur l'initiative européenne GAIA-X, qui doit permettre à l'Europe de retrouver une forme de souveraineté sur le segment du *cloud*. Enfin, mon dernier sujet ne vous étonnera pas au regard de l'actualité très récente, à savoir la vague de cyberattaques sur les systèmes d'information d'établissements de santé. Face à la sophistication de la menace cyber, comment pensez-vous qu'il soit possible de garantir un niveau de protection maximale de nos infrastructures numériques, en particulier dans le domaine de la santé qui est un domaine critique par nature ?

M. Adrien Parrot, président de l'association InterHop. Je suis médecin anesthésiste-réanimateur et informaticien. J'ai travaillé deux ans aux Hôpitaux de Paris, à l'entrepôt de données de santé – une plateforme qui regroupe l'ensemble des données des hôpitaux à des fins de recherche essentiellement. En guise de préambule, je souhaite souligner que l'association InterHop n'est en aucun cas opposée à la recherche en santé. J'en veux pour preuve que j'ai travaillé à l'entrepôt de données de santé de l'AP-HP, qui fait de la recherche. La question n'est pas là. De la même manière, en ce qui concerne le traitement des données, nous sommes conscients de la nécessité que les données ne soient pas accaparées, mais au contraire partagées. InterHop est le diminutif d'« interopérabilité », avec un H pour « hôpitaux ». L'interopérabilité des systèmes d'information est au centre de notre démarche. L'interopérabilité des informations permet d'échanger des informations, au besoin, entre systèmes d'informations différents. La problématique du HDH et de notre combat, par exemple au Conseil d'État, réside dans la protection des libertés fondamentales. Nous agissons exclusivement sur ce terrain. Encore une fois, nous ne sommes pas opposés à un projet de recherche, comme pourrait l'être le HDH. Le HDH est emblématique d'une problématique systémique, avec plusieurs composantes : une centralisation extrême des données, qui s'oppose par exemple au Ouest Data Hub dont vous a entretenu le Pr Marc Cuggia. Dans ce modèle, les projets peuvent être centralisés mais ils le sont au cas par cas, projet par projet, sans que cela ne devienne la norme : autrement dit, toutes les données ne sont donc pas stockées au même endroit, sur une même plateforme. Enfin, ce sont avant tout les problématiques de Microsoft et de l'extraterritorialité du droit américain qui nous ont alertés.

Concernant les alternatives, outre le Ouest Data Hub ou l'AP-HP, centre dans lequel j'ai travaillé, il existe également des entrepôts de données de santé à Marseille, Toulouse, Bordeaux, Lille, Grenoble – et j'en oublie. Les alternatives sont multiples. Pour revenir à l'exemple de l'AP-HP, son entrepôt de données de santé traite plusieurs millions de données de patients (10 à 11 millions sur le site de l'entrepôt de données de santé) avec une plateforme issue des logiciels *open source*. Quand je faisais encore partie de l'équipe, l'autonomie numérique était pensée grâce au logiciel *open source*, celui-ci permettant d'être autonome et de protéger au maximum les données confiées.

L'AP-HP a par ailleurs plusieurs dizaines de projets en cours, sur le Covid-19 actuellement. Si nous voulons aller vite et que nous partons du principe – ce qui est vrai – que le traitement des données et la recherche vont améliorer la qualité de vie et le soin, alors autant renforcer l'existant, que ce soit avec l'AP-HP ou Ouest Data Hub – je n'ai pas de parti pris sur une plateforme en particulier. D'autres alternatives existent. En dehors du secteur public, le Pr Marc Cuggia a parlé du TeraLab tout à l'heure. Le Centre d'accès sécurisé aux données (CASD), qui est homologué au Système national des données de santé (SNDS) et qui possède la certification Hébergeur de Données de Santé (HDS), va jusqu'à proposer des boîtiers physiques où l'utilisateur doit mettre son empreinte digitale pour accéder aux données. Ce système a la qualité de ne pas déporter la sécurité sur le poste utilisateur, celui-ci étant par ailleurs également sécurisé *via* l'infrastructure. Le boîtier se connecte ensuite à une plateforme, qui peut être une plateforme *big data*.

Pour finir, je dirai que les critiques sont nombreuses. Elles ne sont pas propres à notre association : la Commission nationale de l'informatique et des libertés (CNIL) et la Caisse nationale de l'assurance maladie (CNAM) ont également émis de telles critiques. Lorsque j'étais encore en poste aux Hôpitaux de Paris, un courrier rédigé par M. Martin Hirsch et révélé par Mediapart avait en outre pointé les risques de perte de confiance des citoyens, des citoyennes et des patients en cas de doute sur l'extraterritorialité, par exemple du droit américain.

Me Juliette Alibert, avocate, membre de l'association InterHop. Je voulais revenir, puisque vous nous posez la question, M. le rapporteur, sur le contexte autour du contentieux qui englobe le HDH. Vous avez rappelé qu'InterHop était membre de SantéNathon et avait porté ce contentieux devant le Conseil d'État. Pour rappeler le contexte, cela me paraît important, le projet HDH est né fin 2018 et a été mis en place début 2019. Nous avons très tôt su que le choix de la solution technique serait porté sur Microsoft, et ce, sans qu'un appel d'offres ne soit réalisé comme Mme Stéphanie Combe l'a rappelé lors de l'audition de ce matin. Un décret devait normalement permettre de régir le traitement des données au sein du SNDS – le périmètre historique de celui-ci étant modifié. Nous étions dans l'attente de ce décret réglementaire pour procéder à la mise en place et au traitement des données au sein du HDH. Cependant, le contexte sanitaire lié à la crise du Covid -19 et l'état d'urgence ont permis, au regard d'un cadre dérogatoire, de « pousser » le droit commun et de mettre en place les projets et les bases au sein du HDH, alors même que le décret réglementaire n'était pas sorti. Une logique inverse s'est mise en place. Je tiens à rappeler que, normalement, les données de santé d'ores et déjà présentes sur le HDH devront être supprimées à l'issue de l'état d'urgence sanitaire, sauf si le décret d'application venait – lors de sa sortie – à les rendre légales et utilisables à l'issue de cette période.

Dans ce contexte, l'association InterHop s'est saisie de la jurisprudence *Schrems* II de juillet 2020. Cet arrêt a fait valoir que le droit américain n'assurait pas, en l'état, un niveau de protection équivalent au RGPD, ce qui a donné lieu à la fin du *Privacy Shield*. Au-delà, l'intérêt de cette jurisprudence réside dans le fait qu'elle a permis l'appréciation concrète, par le juge européen, des pratiques de renseignement des services américains, sur le fondement notamment de deux bases légales intéressantes : la section 702 du *Foreign Intelligence Surveillance Act* (FISA), qui permet l'obtention immédiate et rapide, par le gouvernement, d'informations très larges, sans aucune notification et sans garantie pour les citoyens européens, et, plus attentatoire aux libertés fondamentales et au droit à la protection des données personnelles, *l'Executive Order 12333*. Ce décret présidentiel autorise, à des fins de renseignement, des techniques d'interception sur les signaux en transit, mais également en dehors des États-Unis, par les câbles sous-marins, ce qui n'est pas sans faire écho aux révélations d'Edward Snowden de 2013.

L'existence de cette collecte large, massive, soumise à la discrétion du gouvernement, sans aucun ciblage et sans autorité indépendante, sans même de droit opposable pour les citoyens européens, s'avère totalement en inadéquation avec le RGPD. Je tiens à le rappeler car, lors des différentes auditions que vous avez pu mener, le *Cloud Act* est souvent évoqué, alors que ces deux bases légales ne le sont pas. Microsoft y est pourtant soumis, en tant que personne morale soumise au droit américain. Il serait donc contraint de transmettre des données si elles lui étaient demandées au titre du *FISA* ou de l'*Executive Order 12333*, et ce, bien que ces données soient conservées sur le territoire européen.

Dans le référé-liberté porté par SantéNathon, dont InterHop est membre, nous avons essayé de faire valoir l'atteinte à cette liberté fondamentale que constitue le droit à la protection des données et à la vie privée, en faisant reconnaître du juge administratif que les risques étaient avérés au regard du *FISA* ou de l'*Executive Order* et que cela constituait une violation des libertés fondamentales. Entre le moment où nous avons déposé le référé et le moment où l'ordonnance a été rendue, un arrêté émanant du ministre de la Santé a été pris le 10 octobre pour interdire le transfert des données vers le territoire des États-Unis. Cependant, nous voulions faire valoir que, indépendamment de ce transfert-là, les données étaient, quoi qu'il en soit, mises en péril de par ces deux textes dont je viens de vous parler. La CNIL l'a très clairement rappelé. Un mémoire en observation a été produit lors de l'audience. Nous sommes donc dans une situation où ces risques ont été reconnus à la fois par le Conseil d'État, puisque

le juge des référés a admis qu'il y avait effectivement des risques, par la CNIL et par le juge de l'Union Européenne, dans l'arrêt *Schrems* II. C'est un élément important qui mérite, je pense, d'être rappelé. Le ministre de la Santé a d'ailleurs lui-même reconnu qu'il existait des risques dans un échange de courriers avec la CNIL. Ces risques existent et sont donc avérés. Dans ce contexte, il nous semble essentiel de défendre les données personnelles des citoyens français comme européens.

Cette audience a également été l'occasion d'aborder les enjeux de sécurité, en particulier la centralisation des données de santé. Il est question ici des données de santé de plus de 67 millions de Français, ainsi que de celles des personnes étrangères soignées sur le territoire français. Il a été rappelé que les clés de chiffrement étaient détenues par Microsoft. Il semblerait d'ailleurs que cette information n'ait pas été démentie dans l'audition que vous avez menée, ce matin. Nous sommes dans une situation où la société Microsoft conserve elle-même les clés de chiffrement. C'est un peu comme si on avait un prisonnier à qui l'on remettait les clés de la cellule. Selon nous, dès lors que les *data scientists* – qui fondent la recherche au sein du HDH – ont besoin d'utiliser ces données, et que Microsoft a accès aux clés de chiffrement, cela signifie que Microsoft déchiffre les données pour permettre la recherche. Or, même si ces données sont pseudonymisées, elles sont ré-identifiables en les croisant entre elles.

M. Adrien Parrot. On voit bien que les enjeux sont moins liés au *Cloud Act,* qu'aux autres textes, de portée extraterritoriale, des États-Unis. On pourrait aussi se poser la question des répercussions, et si cela ne reste qu'un risque. Sur ce terrain, il faut déjà dire que cela ne concerne pas uniquement le terrorisme. J'en veux pour preuve M. Frédéric Pierucci, ancien cadre d'Alstom, qui s'est fait arrêter aux États-Unis et a passé plusieurs mois dans un quartier de haute sécurité, parce que l'État américain avait eu accès à des données provenant de ses mails. C'est bien la portée extraterritoriale du droit américain qui a des répercussions et qui fait pression sur les entreprises – françaises, en l'occurrence. Nous ne parlons pas que du terrorisme, mais de l'intelligence économique au sens large. Il ne faut pas être naïf : les données de santé constituent aussi des enjeux économiques importants. À titre d'exemple, l'investissement sur les données de santé compte pour un tiers du budget « santé » d'Alphabet, la maison-mère de Google.

Concernant les enjeux autour des données de santé, plus précisément, le logiciel libre a pour principe central l'autonomie des utilisateurs et des utilisatrices. Ces derniers peuvent lancer le logiciel directement sur leur poste de travail. Avec l'arrivée du *cloud* et des serveurs distants, cette autonomie s'effrite progressivement, heurtant de plein fouet les enjeux liés aux données de santé. L'un des principes fondateurs de la médecine réside dans le serment d'Hippocrate, autrement dit dans le secret médical. On sait qu'il n'y a pas de confidence sans confiance, et que le secret permet de créer une relation de confiance entre le médecin et le patient. En parallèle, les données doivent être utilisées à des fins de recherche. Les données constituent en quelque sorte l'or du 21ème siècle, dans la mesure où les algorithmes d'intelligence artificielle, les réseaux de neurones, apprennent grâce aux données. Nous avons donc besoin de traiter des données. Cela n'est pas nouveau : la recherche les utilise depuis plusieurs années. Nous sommes confrontés à une balance bénéfices/risques, où il faut faire de la recherche tout en conservant un cadre de sécurité pour ne pas faire peur, pour garder la confiance millénaire, pluri-centenaire, de la relation médecin-malade. Cet enjeu de confiance est central.

Je vais citer une phrase, relative au développement des plateformes, du rapport de la mission présidée par M. Éric Bothorel : *« les infrastructures nécessaires à la donnée sont de plus en plus exposées à des formes de dépendance logicielles, ce qui soulève un enjeu*

d'autonomie stratégique. Il ne faut surtout pas que le patient ou la patiente soit pris dans des enjeux d'autonomie et perde confiance dans le système. Les retentissements en termes de santé publique peuvent aussi être importants sur ce terrain-là ».

Me Juliette Alibert. Pour compléter ces propos, je pense qu'il faut aussi parler des risques majeurs en termes de mise à mal de la Sécurité sociale. On voit bien, aujourd'hui, que les GAFAM – Google, Apple, Facebook, Amazon et Microsoft – et d'autres entreprises privées ont compris l'intérêt financier majeur que les données représentent. L'exemple de la maison mère de Google, Alphabet, qui investit plus de 30 % de son budget dans les données de santé, illustre bien cette prise de conscience. Or, les pratiques des entreprises privées pourraient mettre à mal le système actuel de la Sécurité sociale, qui repose sur une collectivisation des risques. Les pratiques de ces sociétés et les outils connectés pourraient en effet permettre aux GAFAM, demain, de cibler très spécifiquement les individus et d'identifier ceux porteurs de risques, au regard de leur profil, menant ainsi à une forme de médecine prédictive. Ce type de pratiques pourrait progressivement mettre à mal le système actuel en faisant reposer le risque sur l'individu et non plus sur la solidarité et le collectif, dans le même esprit que le principe « pollueur payeur ». Nous pensons que le risque de délitement de la Sécurité sociale constitue l'un des enjeux majeurs des données de santé.

M. Adrien Parrot. Nous avons vu le cadre, à savoir la portée extraterritoriale du droit américain ainsi que les enjeux autour des données et de la santé numérisée. Nous souhaitons maintenant enchaîner sur les solutions que nous espérons modestement apporter. Concernant la gouvernance, nous pensons que l'erreur originelle du HDH est d'avoir fondu la technique et la gouvernance. Nous sommes d'accord pour avoir plutôt une gouvernance centralisée. Nous partageons le constat de la complexité de l'accès aux données et sommes favorables à un guichet unique d'accès, comme se propose de l'être le HDH, avec des facilitations d'accès pour les chercheurs et des publications de cahiers des charges pour que les acteurs du numérique, par exemple, puissent être au courant de ce qui est en train de se passer. Nous ne sommes pas non plus opposés à une plateforme centralisée de gestion des consentements. Des améliorations méritent effectivement d'être apportées à ce niveau. Sur la gouvernance, et pour partir de l'existant, nous pensons qu'il faut créer le plus rapidement possible un comité de pilotage indépendant et multipartite, avec des utilisateurs publics et privés – les pouvoirs publics et les acteurs du numérique – pour engager ces travaux de réversibilité. J'ai appris ce matin que la direction interministérielle du numérique (DINUM) a réalisé une étude sur le sujet. Au titre de nos actions, nous avons demandé l'accès aux rapports de réversibilité. À ce jour, nous avons uniquement pu voir le premier rapport, datant de novembre 2019, mais pas le deuxième. Je pense que ce rapport doit être public et « auditable » par les experts comme par les citoyens.

D'un point de vue technique, c'est un petit peu plus compliqué. Nos propositions consistent à centraliser le développement de codes. Ce mouvement est d'ores et déjà à l'œuvre avec l'existence des forges logicielles (GitLab, GitHub, etc.), qui permettent le regroupement des codes et la collaboration des développeurs sur ces codes. Cette plateforme peut être française ou européenne. Elle permet uniquement de développer des logiciels qui utiliseront les données, sans qu'elle n'ait jamais accès à ces données. Il s'agit donc seulement de développement de code, sur ce principe plutôt centralisé – français ou européen. Par contre, nous sommes radicalement opposés – et nous sommes rejoints, je pense, par le Ouest Data Hub sur ce point – à la centralisation dans les données ou à la centralisation *a minima*, projet par projet. Nous sommes favorables en revanche à la fédération d'acteurs. Cela représente, pour nous, l'application du RGPD. La décentralisation permet de restreindre l'accès aux données à des finalités – une plateforme n'a pas accès à tout, en permanence – et la fédération

permet de répondre aux enjeux d'interopérabilité et de portabilité des données. Ainsi, nous répondons très bien au RGPD avec cette décentralisation technique.

Dernière chose, nous proposons un réseau de fédérations d'ingénieurs avec Inter-CHU, qui regroupe les ingénieurs des hôpitaux français. Ces derniers se réunissent dans ce cadre pour échanger autour de leurs pratiques. Il ne s'agit en aucun cas d'échanger des données, évidemment, mais bien des pratiques – autour du code, par exemple.

Me Juliette Alibert. Nous voulions aussi vous présenter rapidement des propositions davantage tournées vers le volet juridique. Dans la lignée de la loi pour la République numérique, qui prône le recours, pour les administrations, au logiciel libre, nous pensons que le logiciel libre répond, de la meilleure manière possible, à l'intérêt général et au service public, si l'on se réfère aux lois de Rolland par exemple. Nous pensons que le législateur a un rôle important à jouer, dans la mesure où la philosophie du logiciel libre est celle qui « colle » le mieux à la philosophie du service public. Nous pensons que le législateur doit augmenter la part de logiciels libres, peut être en imposant une part obligatoire dans différents secteurs et notamment en matière de santé. Nous souhaitons une exigence particulière dans ce domaine et que tout ce qui relève de la santé soit principalement porté par des acteurs du logiciel libre. Cela permet aussi une protection efficace des données de santé, qui sont des données particulièrement sensibles.

Nous pensons aussi qu'il faut renforcer la certification HDS. Alors que nous étions sous une forme d'agrément, nous sommes récemment passés sous la forme « certification », avec plusieurs niveaux. Dans les différentes auditions menées par votre mission d'information, certains intervenants ont émis des propositions de label. Nous pensons au contraire que le label n'a pas une valeur juridique assez contraignante. Nous souhaiterions plutôt renforcer l'existant en introduisant, par exemple, des clauses spécifiques restreignant le traitement et la sous-traitance des données de santé – parce que c'est ce qui nous intéresse et qu'il s'agit de données particulières, sensibles, prisées – à des acteurs européens *a minima*, permettant d'exclure de fait tous les acteurs hors de l'Union Européenne. Par contre, il serait nécessaire de mener une analyse comparée, notamment au niveau européen, en matière de droit de la concurrence. Bien que cela demande un peaufinage un peu plus important, nous espérons que des travaux seront conduits dans ce sens. Et cela ne peut pas se faire, de notre point de vue, par un label qui n'a pas assez de force coercitive pour garantir l'ensemble de ces conditions.

La troisième proposition juridique que nous souhaitons formuler consiste à renforcer les pouvoirs de la CNIL. Nous voyons aujourd'hui que son budget est largement moins important que celui de la CNIL allemande. Il s'agit donc de la renforcer dans ses moyens, mais également dans ses avis. Aujourd'hui, la CNIL rend des avis, dans le cadre d'un « droit souple ». Autrement dit, ces avis sont de l'ordre de la recommandation et de la préconisation en matière réglementaire, mais n'ont pas de force contraignante. Il ne s'agit pas d'avis conformes. Or, s'agissant de terrains particulièrement sensibles, comme celui les données de santé, il serait peut-être nécessaire d'imposer un cadre d'avis conformes pour ces données. Cela fait partie de nos recommandations.

Enfin, nous sommes persuadés que l'enjeu se joue au niveau européen. Le *Privacy Shield* a fait l'objet d'une annulation par l'effet de la jurisprudence *Schrems* II en juillet dernier. Nous pensons que les négociations doivent être menées de façon particulièrement stricte au niveau européen pour ne pas avoir un nouveau *Safe Harbor* ou un nouveau *Privacy Shield*. Nous voudrions que la gouvernance européenne se saisisse bien de ces enjeux, au regard de ce qui a pu être mis en exergue par le juge européen sur les pratiques actuelles des renseignements américains. Il est important de se rendre compte qu'il n'y a pas de protection

équivalente et qu'on ne peut pas s'en remettre simplement à une nouvelle habilitation de la Commission européenne.

M. Philippe Latombe, rapporteur. Je souhaiterais vous demander quelques précisions dans la mesure où cette audition est publique et doit permettre d'éclairer les gens qui nous écoutent, qui ne sont pas forcément experts du domaine. Aujourd'hui, vous avez mélangé – parce que c'est votre avis – la souveraineté, avec le HDS et le fait que le *cloud* de Microsoft soit utilisé par le HDS, et le logiciel libre. Si nous avions une solution qui ne relève pas du logiciel libre, mais qui soit une offre possible de *cloud* souverain, cela vous conviendrait-il quand même ? Si le HDH n'avait pas utilisé Azure mais OVH, par exemple, seriez-vous allés au Conseil d'État de la même façon ?

Ensuite, et c'est ma deuxième question, le logiciel libre nous assure-t-il de ne pas passer à côté des innovations dans l'avancée technologique, notamment de l'intelligence artificielle, du *machine learning* ou des réseaux neuronaux ? Sommes-nous sûrs que cette solution permettrait d'aller le plus vite possible tout en étant en permanence au bon niveau de l'état de l'art ? Je voudrais séparer les deux questions parce que vous les avez liées. Peut-on les prendre une par une ?

Me Juliette Alibert. Nous avons fait valoir une atteinte au droit à la protection des données devant le Conseil d'État. Si le choix ne s'était pas porté sur une solution technique américaine, je pense que nous n'en serions effectivement pas arrivés là. Pour autant, nous ne sommes pas en faveur d'une hypercentralisation des données. Au contraire, nous sommes favorables à un système reposant sur l'existant – sur les entrepôts de données de santé – et fédérant davantage les acteurs, dans la mesure où nous pensons que la centralisation des données fait reposer sur les données des enjeux de sécurité. En effet, en cas de faille de sécurité, l'ensemble des données de santé des citoyens – Français, Françaises et citoyens étrangers sur le sol français – peuvent devenir accessibles. Nous ne sommes donc pas favorables à ce type de solution et d'organisation du traitement des données de santé en matière de recherche. Nous pensons plutôt qu'il faut fédérer et travailler à des échelons décentralisés. À l'évidence, les risques sont moindres dans le cadre d'une solution européenne portée par un acteur français ou par un acteur européen.

M. Adrien Parrot. Une étude d'IBM pointe le fait que le *hacking* provient, pour 60 %, des organisations en interne. Évidemment, plus on concentre des données dans un point et plus il y a de risques. Ce risque existe vraiment. Ce qui peut être fait, au final, en matière de centralisation, c'est peut-être d'avoir une plateforme pour centraliser certains projets. C'est ce que fait aussi le Groupement de Coopération Sanitaire Hôpitaux Universitaires du Grand Ouest (HUGO). Certaines données sont parfois centralisées à Nantes, sans que cela ne devienne pour autant la norme. Ce qui nous dérange clairement, c'est la dépendance au droit américain. Pour moi, en tant que médecin et au regard du secret médical, les révélations d'Edward Snowden, l'affaire Pierucci ou le FISA sont autant d'éléments qui scellent un *« no go »* absolu.

Concernant la deuxième question, je dirais que les logiciels libres et *open source* nous permettent d'atteindre l'état de l'art. C'est uniquement grâce au logiciel *open source* que nous sommes à l'état de l'art. Toute la plateforme technique de l'AP-HP repose sur des logiciels *open source*. Microsoft en utilise aussi. Il y a deux différences : qui exécute ce code ? – s'il s'agit de serveurs que l'on possède, cela change tout – et est-ce qu'il y a des interfaces de programmation (API), des couches qui englobent le logiciel *open source* ? Par exemple, Microsoft enveloppe un logiciel développé par la communauté, parfois même en partie par lui-même, au sein d'API propriétaires qui emprisonnent l'utilisateur. Aujourd'hui, les projets

sont énormes et mondialisés et, pour collaborer, ceux qui fonctionnent sont presque essentiellement liés au logiciel *open source*.

M. Philippe Latombe, rapporteur. Je reviens sur l'audition précédente des représentants du Ouest Data Hub. Ils nous ont expliqué qu'ils rencontraient une difficulté assez particulière quant aux données et à la certitude que les données soient de bonne qualité et que les mêmes référentiels soient utilisés d'un entrepôt à l'autre – ils citaient par exemple les données de biologie –, dans la mesure où ils ont pu constater des problèmes d'harmonisation. Ils ont indiqué être parvenus à le gérer en raison de leur taille suffisamment importante, mais également grâce à leur histoire et grâce à un mode de fonctionnement très collaboratif entre eux, entre CHU de l'Ouest qui se connaissaient bien. On peut l'entendre aussi au niveau de l'AP-HP, où un certain nombre de discussions ont lieu entre les différents hôpitaux. Le fait de fonctionner de façon décentralisée, avec des entrepôts dans chacun des CHU, qui soient ensuite regroupés sous une forme régionale, avec l'équivalent d'un Ouest Data Hub pour chacune des régions, puis sous une couche nationale et éventuellement une couche européenne, ne générerait-il pas des difficultés sur la qualité de la donnée ?

M. Adrien Parrot. La qualité de données passera nécessairement par la localité, et donc les hôpitaux, peut-être même le cabinet du médecin généraliste. Si on veut faire des traitements de données de qualité, on est obligés d'être très proches du contexte de recueil des données et de comprendre comment les informations sont saisies. Parfois, les systèmes d'information sont tellement mal faits que le médecin entre la donnée où il peut dans son système, mais elle n'est pas forcément au bon endroit. Nous avons donc besoin d'être très proches des chercheurs qui veulent avoir accès aux données. Nous devons savoir à quoi ils ont besoin d'avoir accès. Le chercheur pourra se diriger vers les soignants, à l'endroit où les données sont stockées, regarder sous quel format elles le sont et poser des questions. C'est ce dialogue local, au plus proche de la recherche, des patients et des soignants, qui permettra d'atteindre une recherche de qualité. Il est indispensable que les données soient qualifiées – et 80 % du travail consistant précisément à la qualification des données. En effet, le fait d'envoyer des données brutes en dehors du lieu de production serait tout de suite beaucoup moins pertinent.

Me Juliette Alibert. Cette question se pose sans doute de la même manière si tout est directement centralisé. Si les données sont mal renseignées à la source, le HDH ou les projets hypercentralisés seraient confrontés aux mêmes difficultés de qualité.

M. Philippe Latombe, rapporteur. Sur la partie juridique, il y a deux aspects dans ce que vous dîtes. On nous dit aujourd'hui, assez fréquemment, que l'utilisation d'un *cloud* américain n'est pas problématique dans la mesure où tout est pseudonymisé, où tout est chiffré, et où l'utilisateur est le seul à détenir les clés de chiffrement. Vous avez dit que, dans l'audition, vous aviez compris que les clés de chiffrement étaient chez Microsoft. Pourtant, d'autres organismes qui utilisent des *clouds* américains avancent qu'il n'y a pas de risque parce qu'ils ont leur propre clé de chiffrement et que, au-delà, le transfert a été interdit et les données sont stockées en Europe. En quoi ces éléments ne vous paraissent-ils pas suffisants ? Ce point fait partie des oppositions que vous avez eues lors de la discussion au Conseil d'État notamment.

Me Juliette Alibert. C'est ce que j'essayais d'expliquer tout à l'heure. Effectivement, les données sont pseudonymisées. Cependant, plusieurs études – nous pourrons vous communiquer les références – démontrent que, dès lors qu'on croise les données, même si celles-ci ne sont pas directement ré-identifiantes, il est en réalité très facile de ré-identifier des personnes, lorsqu'on dispose d'informations telles que la localisation, l'âge, le sexe, etc.

Sur l'aspect chiffrement, je tiens à rappeler que nous nous sommes appuyés sur un avis de la CNIL, datant du 20 avril 2020. La CNIL a avancé, dès le début, qu'il y avait plusieurs risques de sécurité importants, notamment sur ces clés de chiffrement détenues par Microsoft. Il nous a été confirmé ce matin – et cela l'avait été lors de l'audience devant le juge du référé – que Microsoft détient bien ces clés. Un système de *« customer lockbox »* permet en théorie un système d'accès sécurisé. Cependant, peut-on remettre les clés à un prisonnier dont on ne veut pas qu'il sorte de sa cellule, et lui dire de ne pas y toucher ? Techniquement, il n'y a aucune modalité qui empêche l'accès aux données par Microsoft. Par ailleurs, dès lors que ces données sont utilisées à des fins de recherche, d'intelligence artificielle – et, encore une fois, nous le rappelons, nous ne sommes pas contre la recherche –, cela signifie qu'elles sont à un moment déchiffrées. Pour permettre à ces *data scientists* de faire leur travail, il faut bien qu'elles soient déchiffrées. Elles leur sont délivrées de façon déchiffrée. La problématique reste donc pleine et entière.

Enfin, concernant l'interdiction des transferts de données vers les États-Unis, nous étions heureux de savoir que, dans l'instruction de notre recours devant le Conseil d'État, le ministre avait effectivement décidé d'empêcher les transferts. C'est une première garantie. Cependant, cela ne modifie pas en substance les risques des citoyens, quant à l'accès à leurs données personnelles sensibles, qui sont les données de leur sphère la plus intime, et vis-à-vis desquelles ils peuvent être victimes de discrimination (par exemple s'ils ont le VIH). Ces risques sont toujours présents, comme l'ont souligné le juge de l'Union européenne, la CNIL ainsi que d'autres acteurs. En tout état de cause, les pratiques du droit américain et ses effets extraterritoriaux ne sont pas conformes, dans le sens qu'ils ne remplissent pas les critères minimums de la protection telle qu'elle est aujourd'hui exigée par le RGPD. Elle ne l'est pas en raison des deux actes que je présentais tout à l'heure : l'*Executive Order*, ce fameux décret présidentiel, et la section *702 du FISA*. Ces deux fondements juridiques permettent aux services de renseignement d'avoir accès, de façon massive, discrétionnaire et indiscriminée, aux données, sans que les citoyens ne puissent s'y opposer d'aucune manière. Aujourd'hui, en tant que citoyen, nous sommes dans un système que nous avons *a minima* choisi : nous avons choisi nos représentants légaux, nos députés, etc. Nous avons accepté d'avoir tout cet ensemble et d'être régis par le RGPD. Cela fait partie du contrat social. Le problème réside dans le fait que des États tiers puissent, en méconnaissance de nos droits et du droit à la protection de nos données, accéder à ces données sensibles. Cela nous semble absolument insuffisant en termes de garantie. Ces pratiques s'inscrivent aujourd'hui en violation du RGPD et, plus largement, du droit à la protection des données, tel qu'il est garanti au niveau européen.

M. Adrien Parrot. Les arrêtés sont protecteurs et nous avons confiance dans la gouvernance du HDH. Cependant, en l'occurrence, Microsoft sera contraint – à son corps défendant – de donner accès aux données, si son supérieur hiérarchique le lui demande, en raison du *FISA* et de l'*Executive Order*. C'est vraiment sur ce point que les garanties sont insuffisantes. Dans ce contexte, nous devons nous interroger : est-il techniquement possible pour Microsoft d'avoir accès à ces données ? Où sont réalisées les analyses ? Le stockage est chiffré. C'est une garantie. Sur quel processeur les analyses sont-elles réalisées ? Est-ce sur un processeur soumis au droit américain ? Ce processeur est-il détenu par Microsoft ? Si le processeur – et c'est le cas – est soumis au droit américain, alors les données ne sont plus protégées.

Quant à la pseudonymisation, on peut toujours, en effet, ré-identifier un individu. Il existe deux techniques principales d'appariement entre bases de données. La première consiste à lier des bases de données à partir d'un même numéro présent dans deux bases différentes (par exemple un numéro de sécurité sociale). En l'absence d'un tel numéro, et si l'on dispose uniquement d'informations telles que l'âge ou le sexe, d'autres techniques permettent de lier

des bases de données entre elles. Ce sont des techniques qui existent, qui sont utilisées en routine. Il est possible de ré-identifier des données de cette manière.

M. Philippe Latombe, rapporteur. Pensez-vous que le recours en Conseil d'État ait pu jouer un rôle dans la position de la CNAM quant à l'interdiction de transférer les données au HDH ? Par ailleurs, percevez-vous des risques équivalents dans d'autres domaines que les données de santé ? Existe-t-il, selon vous, une sorte de « HDH » dans d'autres domaines, pour lesquels le HDH pourrait servir de jurisprudence, d'exemple, si nous devions intervenir ?

Me Juliette Alibert. Je pense effectivement que les réserves de la CNAM sont en lien avec cette mobilisation autour de la protection des données et le recours en Conseil d'État. Le collectif SantéNathon représente de nombreuses personnes de la société civile, des associations de patients, des syndicats de médecins mais également des personnalités ayant travaillé sur la santé. Ces personnes ont soutenu le recours dans la mesure où les enjeux en présence sont importants. En effet, sous couvert d'urgence en lien avec le Covid, et pour aller vite, une solution technique comme Microsoft – qui était présentée comme la plus avantageuse et la seule solution – a été choisie, alors qu'elle met en péril les données de santé. Cela a donné lieu à de nombreux articles de presse et à de nombreuses prises de position dans les médias. Le collectif et le recours ont permis de mettre en lumière l'importance des risques, même s'ils avaient déjà été préalablement dénoncés par plusieurs personnes. Nous restons modestes dans notre démarche. Il est clair que plusieurs personnalités avaient pris position pour dénoncer ces risques importants. Cependant, cette mobilisation du collectif et ce recours ont – je pense – contribué à nourrir les inquiétudes, à faire émerger l'idée que nous étions peut-être allés trop vite, que nous n'avions peut-être pas vérifié si des solutions plus sécurisées étaient possibles, si la gouvernance ne pouvait pas être revue, ce qui a donné lieu à ses réserves de la part de la CNAM, mais également de la CNIL et d'autres autorités indépendantes qui se sont positionnées.

M. Philippe Latombe, rapporteur. Dans le collectif, vous qui avez porté ce recours devant le Conseil d'État, comment percevez-vous l'avenir du HDH ? Pensez-vous que la CNAM va obtempérer et transmettre ses données à terme ? Cela signifie-t-il que les données doivent être transférées très rapidement vers un *cloud* souverain ?

M. Adrien Parrot. La CNAM est historiquement très proche du SNDS. J'ai plutôt confiance dans les prises de position de la CNAM, dans les prochains jours et les prochaines semaines. En effet, l'idée consiste à ne pas bloquer le système ni la recherche. Je pense que tous les travaux qui ont été engagés sur la gouvernance, les travaux légaux, la loi de 2019 sur l'extension du SNDS, doivent être poursuivis et repris. C'est un travail indéniable, qui est tout à fait respectable. Par contre, en ce qui concerne l'hébergeur, notre souhait est que Microsoft s'arrête au plus vite. Les alternatives existent. Si nous ne voulons surtout pas d'interruption, nous pouvons nous tourner vers le CASD, vers Ouest Data Hub pour centraliser un projet de recherche dans les infrastructures – ils savent le faire –, vers l'AP-HP ou encore vers des industriels. En tout état de cause, le savoir de traitement des données est déjà actif, au moins au sein des hôpitaux. La CNAM sait aussi traiter des données. Je suis sûr que, si nous demandons de l'aide à l'existant pour centraliser les données sur certains projets, nous pourrons rentrer dans un cadre protecteur, en l'espace de deux secondes, sans que l'activité ne soit interrompue. Il est important d'avoir conscience que nous sommes dans un *no man's land* juridique, dès lors que nous faisons appel à des sociétés de droit américain. Actuellement, la jurisprudence *Schrems* est en cours, et on n'en mesure pas encore toute la portée. Dans ce contexte, il me paraît déraisonnable de faire courir un risque important aux personnes alors que de nombreuses alternatives existent.

M. Philippe Latombe, rapporteur. Selon vous, la réversibilité est donc faisable rapidement : cette réversibilité pourrait être accomplie, certes en mode peut-être un peu dégradé, dans le sens où elle « n'embarque pas » la totalité de ce qui était prévu au départ par le HDH, mais plus rapidement que le délai annoncé de dix-huit à vingt-quatre mois.

M. Adrien Parrot. Oui. Pour moi, il suffit de décider. Les plateformes fonctionnent. Si on décide de renforcer l'existant, l'existant existe. C'est presque de l'instantané. La sécurité nécessite effectivement d'être renforcée. Cependant, les travaux de sécurité ont d'ores et déjà été initiés. Les hôpitaux n'ont pas attendu le HDH pour renforcer la sécurité, surtout dans les entrepôts de données de santé qui sont des concentrateurs, à leur niveau, de données. L'exemple que je le connais le mieux est celui des hôpitaux de Paris. Sur la sécurité, la plateforme libre de l'AP-HP a subi des audits de sécurité et des tests de pénétration de plateforme. Tout cela est déjà en cours.

Me Juliette Alibert. Nous avions posé la question lors de l'audience devant le Conseil d'État. Nous avions demandé quel était l'état des travaux et des bases implémentées au sein du HDH. À ce moment, je crois que seules trois bases étaient implémentées et qu'aucun projet de recherche n'était versé. En tout état de cause, il s'agit uniquement des données de santé de recherche en lien avec le Covid. En termes d'opportunité de favoriser une réversibilité rapide, je pense donc que nous sommes justement dans le bon *timing*. Il est nécessaire de se saisir de l'occasion avant que d'autres bases ne soient versées sur la plateforme.

M. Philippe Latombe, rapporteur. Ce n'est pas ce qui a été dit ce matin lors de l'audition du HDH. La CNIL a par ailleurs annoncé qu'un délai de 18 à 24 mois serait nécessaire, en ligne avec le ministère de la Santé. Une divergence en terme de temporalité apparaît ici nettement.

M. Adrien Parrot. Il est certain qu'une plateforme centralisée, comme peut la faire Microsoft actuellement et le HDH, nécessite des développements et du temps. Par contre, si l'idée consiste à ne pas bloquer la recherche, il est possible de la poursuivre dans des solutions un peu dégradées, en attente de cette infrastructure. Le CASD ou le TeraLab constituent d'excellents exemples de plateformes « clés en main », qui sont disponibles pour faire des tests et pour avancer. Je pense que c'est le bon moment pour enclencher la réversibilité avant que les projets ne soient trop avancés, en utilisant l'existant. Pour moi, les délais annoncés sont trop importants.

M. Philippe Latombe, rapporteur. Au-delà des données de santé, d'autres domaines sont-ils selon vous confrontés aux mêmes problématiques ?

Me Juliette Alibert. Je pense que la problématique se pose dans tous les domaines faisant appel à des données sensibles au regard des publics qu'elles touchent. On peut, par exemple, penser à l'Éducation nationale. On peut penser à des données relatives à des personnes qui peuvent être exposées à des discriminations importantes, par exemple, des données sur des personnes qui sont en prison. Dans le secteur de l'éducation, le même niveau d'exigence devrait être appliqué, dès lors qu'il s'agit de données portant sur des mineurs.

M. Adrien Parrot. Il s'agit en effet d'un problème systémique. Encore une fois, la portée de la jurisprudence *Schrems* n'est pas encore dévoilée en entier. Nous savons cependant qu'elle concerne les données personnelles de façon large et que tous les secteurs sont touchés. Les enjeux d'intelligence économique sont très larges. Ils s'étendent, par exemple, à la R et D de nos entreprises pharmaceutiques et au développement des vaccins. Ce problème doit être traité dans une dimension systémique, qui dépasse largement la santé.

M. Philippe Latombe, rapporteur. Quelles seraient ou quelles sont vos attentes vis-à-vis du législateur dans le domaine des données de santé ? Certaines choses sont-elles aujourd'hui insuffisamment claires ? Certaines choses nécessiteraient-elles que l'on puisse légiférer ? Est-ce d'abord du domaine du législateur ? Vous avez dit tout à l'heure qu'il faudrait que la CNIL puisse rendre des avis conformes sur un certain nombre de sujets. Certainement, cela relève du législateur. C'est à nous de pouvoir l'imposer. Souhaitez-vous attirer notre attention sur d'autres sujets appelant, selon vous, des évolutions ?

Me Juliette Alibert. Le fait de permettre à la CNIL de rendre les avis conformes sur des données particulièrement sensibles fait effectivement partie de nos propositions. L'une de nos propositions consistait à interdire le traitement des données sensibles – et notamment des données de santé – par des acteurs extra-européens. Nous ne souhaitons pas que le traitement des données s'effectue dans le cadre d'un label, parce que nous sommes convaincus que la sécurité et la force contraignante d'un label n'offrent pas des garanties suffisantes. Il s'agirait plutôt d'un cadre de certification/agrément, ce qui relève en l'occurrence du pouvoir réglementaire. Cela pourrait donc éventuellement passer par une loi, en faisant valoir le caractère spécifique de ces données. Par contre, il faudrait effectivement croiser cette approche avec le droit de la concurrence au niveau de l'Union européenne.

Nous avons également émis une proposition consistant à imposer davantage de logiciels libres dans les administrations, et notamment dès lors que des données de santé sont en jeu. Il est possible, dans ce domaine, d'aller au-delà de la loi pour une République numérique de 2016, avec peut-être des quotas plus importants. En tout état de cause, on sent bien qu'un changement philosophique important est actuellement à l'œuvre. Une mairie – Échirolles, je crois – s'est récemment engagée à mettre en place des solutions de logiciels libres. Je pense vraiment que les services publics et les administrations ont tout intérêt à reposer sur ce type de solution beaucoup plus éthique, où effectivement les données sont protégées (personne n'a accès en clair aux données) mais où une transparence est faite sur le code. Le citoyen peut savoir dans quel cadre ses données sont sécurisées ou non. La lisibilité du code donne énormément d'informations. Ces solutions offrent donc un cadre éthique à la fois très protecteur et très transparent. C'est pour cette raison que nous souhaitons que le législateur légifère en ce sens.

M. Philippe Latombe, rapporteur. Des annonces ont été faites la semaine dernière concernant la création d'une mission sur le logiciel libre au sein de la DINUM, issue de la mission Bothorel. Nous suivrons ce qui en découle. Je souhaite maintenant vous poser la même question que la précédente, mais au niveau européen. Qu'est-ce qui, selon vous, relève du domaine du législateur ou du domaine réglementaire national, et qu'est-ce qui relève – ou pourrait être amélioré – au niveau européen ?

Le combat que vous avez porté auprès du Conseil d'État est issu d'une jurisprudence de la Cour de justice de l'Union européenne, qui invalide le *Privacy Shield* par *Schrems* II. Vous proposez une solution qui serait *« RGPD by design »* et donc décentralisée, en affirmant que cette solution est la plus proche de l'esprit du RGPD, qui constitue lui-même une réglementation d'origine européenne. Que faudrait-il changer, que faudrait-il améliorer au niveau européen sur les données de santé ? Pensez-vous qu'il manque un cadre ?

Me Juliette Alibert. Je pense que le législateur européen doit effectivement réfléchir à aller éventuellement au-delà du cadre du RGPD, notamment sur des données particulièrement sensibles. Un cadre existe et il est très protecteur. Cependant, dans la perspective d'un éventuel futur *Privacy Shield*, les négociations empêchent peut-être la reconnaissance d'un niveau de protection équivalente. En ce qui nous concerne, nous sommes

plutôt opposés à ce type d'accord. Il s'agit de notre positionnement militant. Cependant, il me semble indispensable que le législateur européen travaille sur ses aspects.

M. Adrien Parrot. Tant que les services de renseignement américains sont ce qu'ils sont, et tant que le droit américain dispose de cette portée extraterritoriale, l'Europe doit rester très vigilante face à l'émergence de futurs textes et se méfier d'un éventuel *Privacy Shield* ou d'un *Safe Harbor III*.

Me Juliette Alibert. Peut-être faudrait-il imaginer, au-delà du RGPD, des directives européennes spécifiques permettant de laisser à chacun des États des marges de manœuvre pour protéger certaines données particulièrement sensibles. En tout état de cause, je pense qu'il y a énormément à faire au niveau européen. L'enjeu que constitue la protection des données personnelles ne peut s'affranchir de cet échelon-là.

M. Philippe Latombe, rapporteur. Concernant la protection cyber des données, vous avez, dans votre propos liminaire, avancé que le fait d'avoir un système centralisé pouvait générer des risques plus importants, dans la mesure où une faille pourrait mener à l'ensemble des données. Un système décentralisé permettrait à l'inverse de ne pas « mettre tous ses œufs dans le même panier ». Comment expliquez-vous les attaques qui surviennent actuellement et comment s'en prémunir ? Faut-il créer un écosystème spécialement dédié aux données de santé, qui soit à la main des directions des systèmes d'information (DSI) dans chacun des CHU – si je prends votre modèle décentralisé ? Faut-il recourir à des solutions privées ?

M. Adrien Parrot. Les DSI ne disposent pas de moyens financiers suffisamment importants pour répondre aux besoins. Elles peinent à obtenir des ingénieurs de qualité en quantité suffisante. La difficulté est en partie liée à cette situation, et c'est typiquement ce que le logiciel *open source* peut faire et peut apporter. L'État – et il s'agit peut-être de l'une des prochaines missions de la DINUM – devra, dans un premier temps, recenser les logiciels existants, mettre en avant un catalogue de logiciels et s'appliquer à « mettre de la glu » entre ces différentes briques logicielles. Cela permettra ensuite de proposer des briques, unifiées dans un tout cohérent, aux hôpitaux et aux professionnels de santé. Ces derniers pourront aider localement à l'installation des logiciels, qui peuvent être certifiés. Le fait d'initier une gouvernance qui fournit du code et du logiciel libre – pour le secteur public, en l'occurrence – semble être une très bonne idée. C'est aussi reprendre ce que pourrait faire Framasoft et ce qui est partiellement fait par l'État, avec son ébauche d'annuaire. Il faut renforcer ces actions, créer des forges logicielles et embaucher des développeurs qui créent des logiciels prêts à être utilisés directement dans les hôpitaux. Ce travail est tout à fait nécessaire. Notre association s'efforce d'œuvrer dans cette direction afin de pallier le manque que nous observons sur ce terrain. Nous essayons ainsi de « mettre de la glu » entre plusieurs logiciels et de les proposer aux professionnels de santé.

M. Philippe Latombe, rapporteur. Souhaitez-vous aborder certains sujets que nous n'aurions pas traités, qu'il s'agisse des données de santé ou de la souveraineté ?

Me Juliette Alibert. En ce qui concerne la souveraineté, je préciserai simplement que nous nous attachons plutôt à une notion d'« autonomie numérique » que de « souveraineté numérique ». En effet, les enjeux de souveraineté relèvent à notre sens de l'autonomisation des acteurs – au sens de la capacité de ces derniers à avoir la maîtrise de leurs données et de leur sphère numérique. Selon nous, les enjeux se situent à tous les niveaux : à l'échelle individuelle, à l'échelle départementale, à l'échelle régionale, au niveau de l'État et, enfin, entre les États eux-mêmes. La souveraineté nous semble trop rattachée à la notion souverainiste des États-nations face aux États tiers, alors même qu'une collaboration est à l'œuvre au niveau européen entre les membres de la Communauté européenne. Pour nous,

cette notion de souveraineté ne fait donc pas nécessairement sens. C'est pour cette raison que nous préférons la notion d'autonomie numérique.

M. Adrien Parrot. C'est en construisant que nous avancerons. Il est nécessaire de coconstruire localement pour produire des données de qualité, ces dernières étant ensuite utilisées par les algorithmes. Il faut donc repartir de la localité et coconstruire des logiciels, peut-être grâce à l'appui de la puissance publique. En tout état de cause, un travail de coconstruction entre les hôpitaux doit clairement être favorisé et animé.

Nous devons par ailleurs bien nous rappeler que le principe du secret médical est au centre de la question du traitement des données de santé. Ce principe est pluri-centenaire et cela me semblerait déraisonnable de renier le serment d'Hippocrate. Nous nous devons de sécuriser les données, et particulièrement les données de santé, sans quoi une perte de confiance des patients est à craindre.

Me Juliette Alibert. Concernant le risque de perte de confiance des patients, il est indispensable de démontrer un niveau d'exemplarité et de transparence important, lors de l'implémentation de projets tels que le HDH. Par exemple, il nous a été dit qu'aucun appel d'offres n'avait été conduit car une solution existait et que les autres solutions n'étaient pas envisageables. Il faudrait pourtant que le citoyen ait accès, de façon transparente, à l'ensemble des documents qui montrent que toutes les solutions existantes ont été auditées, et qui expliquent pour quelle raison le choix s'est porté sur cette entreprise plutôt qu'une autre. Il est nécessaire que le choix soit *a minima* expliqué. Il a été indiqué ce matin que le choix se porterait de nouveau sur Microsoft si un marché public venait à être reconduit. Or, nous n'avons pas les moyens de comprendre ce choix en tant que citoyens. Nous avons pourtant besoin de comprendre les décisions politiques pour y adhérer, notamment lorsque ces décisions mobilisent des enjeux de sécurité importants. Je pense qu'il est indispensable de donner les clés de lecture aux citoyens. L'association InterHop a en outre soumis des demandes d'informations concernant plusieurs documents annoncés comme « publics » sur le site de la DINUM. Or, nous peinons à y accéder. Je ne dis pas que nous nous heurtons à une mauvaise volonté de l'État de nous fournir ces documents, mais simplement qu'il sera difficile de comprendre les choix qui sont faits en l'absence d'une plus grande transparence. Cette lisibilité est cruciale dans la mesure où nous ne pouvons pas transiger avec les libertés individuelles, ni avec le droit au secret médical. Il est clair qu'on ne peut pas avoir recours à ces solutions en méconnaissance des libertés fondamentales, et d'autant plus quand aucune explication n'est fournie et quand l'accès à certains documents clé qui permettraient de comprendre et de réfléchir de façon concertée – en réunissant, en terme de gouvernance, des associations de patients – n'est pas communiqué. Je pense que les choses ont été très rapidement exécutées, alors qu'on avait peut-être le temps pour prendre des décisions. Ces dernières ont été rapidement mises en place, et ce, alors même que nous n'étions pas encore dans l'urgence du Covid. En effet, le choix de Microsoft a été opéré en amont de la crise sanitaire, et non pour y répondre.

M. Philippe Latombe, rapporteur. En tant que rapporteur, je serais preneur de la liste des documents publics auxquels vous avez demandé d'avoir accès, mais que vous n'avez pas obtenus. Cela m'intéresserait, en tant que parlementaire, que vous puissiez me la faire parvenir dans la note écrite que vous nous transmettrez.

Me Juliette Alibert. Bien sûr.

Audition, ouverte à la presse, de M. Benoît Darde, administrateur de Syntec Numérique
(25 février 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons aujourd'hui M. Benoît Darde, administrateur de Syntec Numérique. Il est accompagné de Mme Philippine Lefèvre, déléguée aux relations institutionnelles, et de Mme Anissa Kemiche, chargée des affaires européennes. Syntec Numérique est une organisation professionnelle rassemblant des entreprises de services du numérique, des éditeurs de logiciels et des sociétés de conseil en technologies. Syntec Numérique regroupe plus de 2 000 entreprises adhérentes, qui représentent environ 90% du chiffre d'affaires de ce secteur d'activité.

Nous souhaitons échanger avec vous sur la façon dont l'écosystème du numérique perçoit la problématique de la souveraineté numérique. Nous sommes évidemment intéressés par votre regard et vos propositions sur la meilleure façon de soutenir le développement de cet écosystème. Nous souhaiterions également aborder le sujet de la numérisation des entreprises françaises, qui constitue un impératif important pour que nos entreprises tirent le meilleur profit de la révolution numérique tout en conservant la maîtrise de leur destin numérique.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

J'aimerais d'abord que vous nous indiquiez ce que recouvre, pour vous, la notion de souveraineté numérique. Ce concept fait l'objet d'une attention croissante de la part des pouvoirs publics, notamment depuis la crise sanitaire. Au cours de nos auditions, nous avons eu l'occasion de recueillir plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. J'aimerais donc savoir comment, en votre qualité de représentant d'une partie de l'écosystème des entreprises du numérique, vous appréhendez cette notion.

Je souhaiterais ensuite vous entendre sur la situation actuelle des entreprises du numérique. J'aimerais notamment savoir comment elles appréhendent cette crise sanitaire qui dure et quelles sont leurs anticipations pour les prochains mois. J'aimerais également vous interroger sur le niveau de maturité de l'écosystème du numérique français et sur ses attentes vis-à-vis des pouvoirs publics. Quels sont, selon vous, nos forces, nos faiblesses et les leviers d'action prioritaires à mobiliser ? Nos précédentes auditions ont fait apparaître des points clés, comme par exemple le rôle de la commande publique, en particulier à destination des petites et moyennes entreprises (PME). Je souhaiterais savoir si vous identifiez d'autres points sensibles et prendre connaissance de vos propositions pour accélérer le développement des entreprises du numérique dans les prochaines années.

Enfin, je souhaiterais vous entendre sur les différents projets à l'œuvre au niveau européen dans le domaine du numérique, notamment avec le *Digital Services Act* ou le *Digital Markets Act*. Ces projets vous paraissent-ils adaptés aux défis que nous devrons affronter ces prochaines années ? Formez-vous des attentes spécifiques sur ces textes, que vous souhaiteriez partager avec nous ?

M. Benoît Darde, administrateur de Syntec Numérique. Je suis *partner* et membre du comité exécutif de la société Wavestone. Par mes activités de conseil, j'accompagne mes

clients, depuis un peu plus de vingt-cinq ans, dans leur transformation numérique. Je suis également administrateur au sein de Syntec Numérique, où je suis chargé notamment d'animer la communication sur le secteur et le marché du numérique. Je préside par ailleurs la commission des relations institutionnelles de Syntec Numérique.

J'ajouterais quelques points à votre brève introduction de Syntec Numérique. Nos 2 000 entreprises adhérentes représentent environ 57 milliards d'euros de chiffres d'affaires en France et 80% des entreprises du secteur du numérique. Elles regroupent un panel d'entreprises varié : des entreprises de services, des entreprises d'édition de logiciels et des entreprises de conseil en technologies. Elles se composent d'une trentaine de très grands comptes, de 150 entreprises de taille intermédiaire (ETI) ainsi que d'un maillage très fin de mille PME, mille start-up et très petites entreprises (TPE) sur tout le territoire. Nous couvrons ainsi l'écosystème sur ses différents métiers et dans ses différentes tailles, et prenons connaissance de ses différents besoins et préoccupations.

Nous espérons que vos travaux permettront de clarifier les débats autour du terme de souveraineté numérique et d'apporter des propositions permettant de renforcer l'écosystème numérique français et européen.

La souveraineté suppose à mon sens trois choses : tout d'abord, un support de financement, ensuite, un cadre réglementaire, et, enfin, des opérations de formation et d'attractivité sur les sujets de la transformation numérique.

La souveraineté suppose tout d'abord un support de financement : comme dans tout projet public ou privé, les ambitions et les lignes stratégiques de développement doivent être soutenues par des moyens. Nous devons déclencher la capacité à encourager davantage l'investissement public et privé vers des technologies de pointe, choisies comme des cibles majeures pour la France et l'Europe, ainsi que vers des sujets plus généraux comme la cybersécurité.

La souveraineté soulève également un sujet d'ordre réglementaire. Disposer d'un écosystème européen fort dans le domaine du numérique suppose de pouvoir mettre l'ensemble du marché européen à disposition de notre écosystème et de construire la capacité de nos acteurs à recourir au marché européen le plus facilement possible. Le marché européen représente environ 500 millions d'habitants : en ce sens, il constitue un bien meilleur terrain de jeu que chaque marché domestique. Plus nous donnerons la possibilité à nos entreprises de se développer rapidement sur l'ensemble du marché européen, plus nous verrons émerger de grands acteurs qui concourront à notre autonomie, à notre performance et donc à notre souveraineté dans le monde du numérique.

Enfin, la formation constitue un vecteur essentiel de souveraineté. Des plans de reconversion importants, intervenant au cours de l'évolution des parcours professionnels des personnes, peuvent amener de nouvelles compétences dans le domaine du numérique. Nous devons également construire l'attractivité du secteur auprès des futures générations. Certaines avancées ont eu lieu en la matière ces dernières années, mais nous devons aller plus loin dans l'attractivité des activités du numérique.

Les États et l'Europe doivent donc continuer à investir dans les nouvelles technologies et favoriser l'accompagnement de tous les secteurs – car le numérique n'est pas seulement constitué par les entreprises que Syntec Numérique représente : le numérique concerne toutes les entreprises. Il faut absolument accompagner la transformation dans tous les secteurs et pour toutes les tailles d'entreprises. Il convient également de répondre à un certain nombre de défis au sujet du numérique, notamment en matière d'inclusion, de mixité et de transition

écologique. Toutes ces conditions garantissent notre propre souveraineté technologique et numérique, et permettront de faire émerger et d'installer durablement des acteurs européens clés qui constitueront des alternatives aux acteurs actuellement en place dans le monde du numérique.

Je répondrai maintenant aux questions que vous avez posées. Je commencerai par faire un point sur la situation actuelle des entreprises du numérique. Le secteur du numérique représente environ 57 milliards d'euros de chiffres d'affaires. Il a connu une très forte croissance ces dernières années, se situant entre trois à cinq points de croissance annuelle. Il a généré un nombre important d'emplois : il a permis 175 000 créations nettes d'emplois ces dix dernières années, dont 23 000 créations en 2019, selon les données statistiques de l'emploi de l'Agence centrale des organismes de sécurité sociale (ACOSS). Ce secteur connaît donc une importante dynamique de croissance, alimentée par les activités du numérique, les réseaux sociaux, les technologies mobiles, les problématiques d'analytique, de *cloud* et de sécurité. Nous rassemblons ces problématiques tractant une forte croissance sous le terme de SMACS (acronyme de *Social – Mobility – Analytics – Cloud & Security*).

Les difficultés, suite à la crise sanitaire, sont réelles. Puisque le numérique a été essentiel pour le télétravail, l'idée s'est répandue dans l'imaginaire collectif que le secteur passait au travers de la crise sanitaire sans encombre, voire en en retirant des contributions positives. Cela n'est pas du tout le cas. Nos prévisions établissaient un taux de croissance d'un peu moins de 5% pour l'année 2020 : en réalité, nous sommes en décroissance de 4,6%. Nous prévoyons un redécollage extrêmement léger, de l'ordre de 1%, de l'ensemble de notre secteur en 2021.

Les fonctionnements diffèrent à l'intérieur du secteur. L'édition de logiciels a plutôt bien résisté à la crise : elle ne connaît pas de décroissance, mais a maintenu un taux de croissance *flat* pendant l'année 2020. Elle repartira plus fortement que les autres en 2021, avec une perspective au-delà de 3% de croissance – cette perspective est inférieure à la dynamique de la croissance de l'édition de logiciels, qui se situait autour de 6% l'année précédente. Les activités des entreprises de services numériques connaîtront une légère reprise de la croissance l'année prochaine. Enfin, les entreprises de conseil en technologies ont été les plus durement touchées pendant l'année 2020 : elles ont subi une baisse d'activité de 7 %. Cela s'explique par le fait qu'elles servent énormément les secteurs de l'aéronautique et de l'automobile, qui ont été durement impactés par la crise sanitaire. En conséquence, nos entreprises de conseil en technologies, sous-traitantes de ces industries, ont été fortement touchées. Leur situation devrait encore être décroissante l'année prochaine.

Évidemment, nous ne sommes pas aussi touchés que l'aéronautique, l'automobile, l'hôtellerie ou la restauration. Néanmoins, nous subissons un réel impact de la crise. Nous sommes passés d'une situation de croissance soutenue à une décroissance structurante au cours de l'année 2020. Nous espérons une reprise aux alentours de 1% en 2021, mais ces perspectives de croissance sont encore assujetties aux évolutions de la crise sanitaire.

J'en viendrai maintenant à la définition de la souveraineté numérique. Nous devons dépasser les débats manichéens. Il est essentiel que l'Union européenne dispose d'un cadre réglementaire propice au développement d'un *leadership* technologique européen à portée mondiale, tout en préservant son attractivité pour des investissements étrangers, afin d'exploiter des capacités d'innovation qui proviennent d'autres pays que les pays européens. Le terme de souveraineté technologique, sur la définition duquel tous les États européens ne se sont pas encore alignés, devrait, à notre sens, renvoyer à l'ambition de retrouver la compétitivité de nos économies. Cela demande d'investir massivement dans les individus et dans les compétences en matière de technologiques numériques. Cette ambition de servir des

économies compétitives au niveau mondial suppose d'investir massivement dans la recherche européenne, pour lui permettre de trouver des débouchés industriels et pour disposer d'un marché européen qui constituera la première base d'émergence et de passage à l'échelle pour les entreprises du secteur.

Nous pensons qu'il faut saisir l'opportunité ouverte par la stratégie numérique de la Commission européenne. Cette stratégie vise à créer les conditions favorables à l'innovation en Europe sans tomber dans le piège du protectionnisme. Il ne faut pas priver les entreprises de leurs perspectives de développement à l'international au-delà des frontières européennes, ni priver les entreprises de pouvoir recourir à des technologies provenant d'autres périmètres. Le protectionnisme ne rendrait donc pas service à la compétitivité ni au développement des entreprises. Nous pensons qu'une entreprise doit développer des services avec une proposition de valeur différenciante et utiliser l'ensemble des technologies et des éléments de compétitivité à sa disposition pour procéder à sa différenciation dans son propre secteur. L'Union européenne ne doit donc pas se fermer à la collaboration avec les autres régions du monde en matière d'innovation et de numérique. Elle ne doit pas non plus réglementer son marché et les activités de toutes les entreprises qui en sont issues. Nous ne devons pas subir de choc lourd de mise en réglementation en Europe qui restreindrait la capacité de développement de nos entreprises. Nous devons trouver un équilibre entre la coopération avec des acteurs internationaux et la capacité à fournir un marché européen pour l'ensemble des acteurs européens, tout en trouvant les moyens de répondre aux attentes des utilisateurs sur le territoire européen. Il ne faut donc pas entrer dans des débats manichéens. Il serait bon de mettre en place des règles et de veiller au respect strict de ces règles sur le marché unique, notamment en matière de distorsion de la concurrence, d'obstacles au marché du numérique et de pratiques commerciales déloyales à l'échelle européenne. Ces règles seraient respectées par tous les acteurs, y compris par les acteurs étrangers qui viendraient travailler sur le marché européen. Ces règles doivent être renforcées afin de mettre en place un environnement économique propice au développement du numérique, lequel constitue, pour nous, la clé de l'émergence d'une souveraineté technologique et numérique.

Je répondrai maintenant à votre question sur le niveau de maturité des entreprises françaises, leurs forces et leurs faiblesses. Si l'on veut créer des champions numériques européens, nous devons continuer à penser en écosystèmes. Il ne faut pas comprendre la souveraineté technologique comme une logique de fabrication de produits de souche européenne, qui seraient constitués à 100% de sujets de souche européenne. Cela n'est pas faisable. À titre d'exemple, nous sommes en train de mettre en place un certain nombre d'investissements publics dans le domaine de l'informatique quantique afin de pouvoir disposer d'un ordinateur quantique opérationnel. Être détenteur d'une telle technologie représente un axe stratégique extrêmement important en termes de souveraineté technologique, c'est-à-dire d'autonomie. Pour autant, il n'est pas nécessaire que cet ordinateur soit constitué de composants exclusivement européens de souche. En revanche, nous devons être autonomes dans notre capacité à *sourcer* les composants dont nous avons besoin pour intégrer cet ordinateur quantique. L'autonomie dans la fabrication des batteries de véhicules nécessite, elle aussi, d'étudier l'ensemble de la filière d'extraction des minerais, et du cobalt notamment. L'autonomie dans la fabrication de l'ordinateur quantique se mesure, de la même manière, par notre capacité à disposer de plusieurs filières de fournitures de pièces électroniques comme les microcontrôleurs. Cela est une manière d'éviter d'être lié et menotté à un seul fournisseur. Créer une autonomie stratégique et une souveraineté technologique suppose donc de se doter de capacités différenciantes sans avoir besoin de tout monter par soi-même. Nous devons donc regarder où se situe notre différence, puis maîtriser notre *sourcing*, c'est-à-dire notre capacité à diversifier nos sources d'approvisionnement.

Nous devons également apporter aux écosystèmes la maîtrise des données sensibles. Il est légitime, pour certaines données, d'avoir recours à des solutions qui proposent des protections supplémentaires en matière d'hébergement, de chiffrement ou même de protection juridique. Cela doit passer par des capacités d'encadrement ainsi que par des services de sécurisation technologique et juridique pour installer ces données particulièrement sensibles, qu'elles soient publiques ou privées.

M. Philippe Latombe, rapporteur. Que sont les données sensibles pour vous ? Parlez-vous des données sensibles au sens du Règlement général sur la protection des données (RGPD), ou cela va-t-il au-delà ? Quelles données devons-nous garder grâce à une protection juridique et technologique suffisante pour éviter leur fuite ?

M. Benoît Darde. Notre compréhension des données sensibles va au-delà de celle du RGPD. Une entreprise travaillant sur sa stratégie et ses éléments différenciateurs dispose d'informations confidentielles et de secrets industriels. Il revient donc à chacune de nos entreprises ainsi qu'à nos administrations de définir les données et les savoirs qu'il faut absolument protéger. Il est nécessaire d'obtenir, pour ces données, des conditions de traitement et d'hébergement qui permettent aux entreprises et aux administrations de garder un avantage compétitif dans chacun de leurs secteurs d'activité. Les données sensibles recouvrent donc un spectre assez large. Elles ne peuvent pas être définies immédiatement : il faut les définir au cas par cas, selon les entreprises et les usages.

La capacité à maîtriser les traitements et l'hébergement des données varie en fonction des structures. À titre d'exemple, une start-up de trente personnes est en train de développer une solution extrêmement pointue et innovante dans une *biotech*, nécessitant l'exploitation de données d'analyses, mais sa capacité à définir les conditions d'hébergement et de sécurisation de son environnement est faible. Comment garantir à cette start-up de bien protéger son *asset*, c'est-à-dire son différenciateur ? L'écosystème est intéressant car il permet de disposer de capacités et d'apporter des garanties à ce sujet à un certain nombre d'entreprises.

À ce titre, GAIA-X définit des modèles avec des protocoles technologiques et juridiques qui proposent des solutions pour garder les secrets des entreprises. Il revient ensuite à chaque entreprise et à chaque administration de définir ses données sensibles. Nous ne pouvons pas définir une donnée sensible *ex nihilo* pour tous. Une réglementation, secteur par secteur, pourrait contribuer à définir des sets de données sensibles, mais je suis méfiant quant à l'idée de légiférer sur ce qu'est une donnée sensible, car une telle définition serait sujette à des interprétations très complexes à traiter ensuite par les entreprises.

M. Philippe Latombe, rapporteur. Pensez-vous que les entreprises françaises sont suffisamment conscientes de la valeur des données comme actifs ou *assets* ? Sont-elles suffisamment informées des risques de sécurité dont elles doivent se prémunir ? Où en est le niveau de maturité des entreprises en la matière ? Je ne parle pas seulement des entreprises innovantes ou des entreprises du numérique, mais bien de l'ensemble des entreprises. Toutes les entreprises sont en effet concernées par les secrets industriels et les secrets de fabrication. Pensez-vous que les entreprises sont aujourd'hui conscientes de la nécessité de protéger leurs données et leurs savoir-faire ?

M. Benoît Darde. La prise de conscience de l'importance du sujet a beaucoup progressé sur le temps récent. Les cas de fuites de données, qui sont relatés quasiment quotidiennement depuis l'obligation de les divulguer décidée par le RGPD, montrent bien l'importance des données. La prise de conscience est donc aujourd'hui réelle.

En revanche, la maturité nécessaire pour savoir comment réagir et comment se prémunir face à ces risques est encore faible. La complexité de ces sujets est forte et la maturité des entreprises en la matière est encore faible. Dans certains épisodes très récents de fuites de données comme SolarWinds ou Centreon, les attaques ont été introduites par des composants logiciels édités par des fournisseurs de solutions et des éditeurs de logiciels. Ces fournisseurs et éditeurs sont attaqués et, sans le savoir, embarquent un code malveillant dans leurs produits. Les clients achètent à ces éditeurs une solution de comptabilité et, quand ils l'installent, ouvrent sans le savoir une faille de sécurité dans leur système. Les acteurs du numérique sont donc conscients que la protection de leurs données est un sujet complexe et important, et qu'il faut absolument, demain, mieux protéger leurs produits, mais leur compétence en cybersécurité n'est pas au niveau de celle des attaquants. À titre d'exemple, la capacité d'une petite entreprise ou d'une start-up élaborant une solution de vidéoconférence à se protéger face à des entreprises criminelles est faible.

L'écosystème a donc encore du travail à faire en la matière. Les travaux avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) doivent être poursuivis. Les investissements en faveur de l'écosystème cyber doivent être renforcés, qui permettront de passer à 40 000 emplois dans le secteur – à ce sujet, nous sommes complètement en ligne avec les objectifs décidés par le Président de la République. Mais cela va prendre du temps.

Nous appelons à disposer de labellisations et de certifications pour apporter de la compétence. Ainsi, les logiciels mis sur le marché qui auront passé un certain nombre de tests bénéficieront d'un label qui garantit la confiance dans le produit. Pour fonctionner, l'économie numérique a besoin de reposer sur de la confiance. Si l'on perd la confiance, on perdra des points de performance dans le développement du numérique, et donc dans l'économie globalement, car le numérique concerne toutes les entreprises. Nous devons absolument travailler à augmenter cette confiance, à mettre en place des systèmes de labellisations et de certifications, et à faire émerger des normes et des standards forts au niveau européen, qui pourront compter mondialement. La normalisation est un sujet central dans la souveraineté technologique de demain. La Chine suit de près ce qui se passe en la matière, s'attache à prendre des positions auprès de tous les acteurs internationaux de normalisation de technologies, voire influence la construction de ces normes. Nous devrions aussi mener ce travail, collectivement et en écosystèmes. Nous devons accompagner l'émergence de normes et de standards européens en matière technologique, pour qu'ils soient alignés avec les pratiques commerciales et de concurrence que nous souhaitons.

Pour conclure, les entreprises sont conscientes des risques, mais elles n'ont pas la maturité nécessaire pour y faire face. Et plus les entreprises sont petites, moins elles sont conscientes de ces risques. La maturité collective en la matière, toutes entreprises confondues, est donc encore faible.

M. Philippe Latombe, rapporteur. Vous avez abordé les enjeux d'éducation dans votre propos liminaire. Quel serait, selon vous, le bon niveau d'éducation en matière de numérique ? Quel socle commun devrait être présenté aux enfants à l'école, et jusqu'à quel âge ? Dans l'enseignement primaire et secondaire, que devrions-nous faire qui manque aujourd'hui ? Quelles sont vos préconisations ou vos pistes sur ce sujet ?

M. Benoît Darde. Nous pensons que notre offre de formation actuelle est de qualité. Elle a évolué de manière très positive. J'en veux pour exemples la création de l'enseignement des sciences numériques et technologiques en classe de seconde générale, la spécialité du numérique et des sciences informatiques en classe de première et en terminale dans les lycées généraux, et la filière mathématiques, physique, informatique et ingénierie (MP2I) dans les classes préparatoires aux grandes écoles. Beaucoup d'avancées ont eu lieu. La capacité de

formation pour le secteur des métiers du numérique, de l'ingénierie et du conseil est satisfaisante. Nous considérons que l'offre est suffisante, à la fois en termes de contenus et de capacités de formation.

En revanche, l'attractivité est insuffisante. La promotion de ces parcours de formation et des métiers du numérique doit être amplifiée. Nous menons des actions, organisons des événements appelés les *Day-Click*, nous intervenons dans les forums métiers des écoles. Il faut augmenter ces actions et leur accorder beaucoup plus de moyens, et des moyens qui soient modernes et « *catchy* » (accrocheurs en français). J'ai vu la dernière vidéo sur les problématiques de cybersécurité inspirée de la série « Le bureau des légendes ». Il faut communiquer sur les réseaux sociaux et montrer à quel point les sujets du monde du numérique sont intéressants et ambitieux. Il faut également expliquer que ces métiers ne sont pas dédiés aux titulaires d'un bac+5 et qu'ils ne sont pas seulement destinés aux hommes. Des moyens doivent donc être déployés pour l'attractivité du numérique – c'est là que le plus grand travail reste à faire. Beaucoup d'initiatives existent à ce sujet, et nous avons tout intérêt à les amplifier. Je salue le programme Femmes du numérique et la fondation Femmes numériques, qui travaillent à faire évoluer les stéréotypes de genre sur le marché de l'informatique et de l'ingénierie en informatique. Nous devons absolument atteindre les différents publics : cela comprend évidemment les jeunes, mais aussi leurs parents. Nous devons travailler à des communications qui les « percutent ». À titre d'exemple, je trouve la communication de l'armée, sur ses métiers, extrêmement intéressante. Nous pourrions nous en inspirer et rendre le monde du numérique, ainsi que le sujet de la cybersécurité, extrêmement attractifs. La cybersécurité n'est pas seulement le stéréotype du garçon en sweat à capuche dans une pièce sombre, assis devant son ordinateur à coder. Faire évoluer cette perception constitue un vrai enjeu.

Cela passera également par la formation et la promotion de l'usage de certains composants numériques pour toute la population. Un classement récent montrait que la France se situait à la 15e place de l'indice 2020 relatif à l'économie et à la société du numérique (DESI). Trop peu de personnes se distinguent, par leurs compétences, dans les technologies du numérique. Je constate que beaucoup de très bons élèves, et notamment les filles, optent pour des parcours dans la santé et fuient le monde du numérique par mécompréhension. Or le numérique est essentiel dans les sciences de santé de demain.

En matière de formation, l'enjeu principal, à mes yeux, est donc de changer l'image du numérique, de montrer qu'il sera demain un des principaux pourvoyeurs d'emplois et que les femmes pourront y être indépendantes, avec des activités bien rémunérées car créatrices de grande valeur.

M. Philippe Latombe, rapporteur. Quel est, selon vous, le rôle de l'État dans le soutien de l'ensemble de la filière du numérique ? À titre d'exemple, la commande publique constitue-elle aujourd'hui un relais suffisant pour les entreprises du numérique ? Des éléments doivent-ils être améliorés ? L'État devrait-il prendre conscience de certains enjeux à ce sujet ?

M. Benoît Darde. Les pouvoirs publics ont pris le parti d'encourager le développement de l'écosystème en France et en Europe. Nous le voyons par un certain nombre d'annonces et de décisions.

L'action des pouvoirs publics, et notamment leur capacité d'investissement, doit encourager l'émergence d'écosystèmes qui va créer un marché et une économie. Le numérique n'a pas besoin de subventions : il a besoin de marchés et d'opportunités de *business*. La puissance d'investissement des pouvoirs publics doit donc faire émerger ces éléments d'écosystèmes et les appuyer dans leur lancement.

Des initiatives d'investissements et d'aides au lancement de ces écosystèmes sont intéressantes. Les verticaux de données sectorielles, par exemple, seront très importants : il est intéressant de poursuivre cette approche portée par GAIA-X. D'autres initiatives doivent être soutenues : l'accès à une donnée partagée et en libre circulation sur notre marché européen, l'innovation dans le domaine de la santé, l'accélération de la stratégie en matière de 5G, les offres de solutions d'intelligence artificielle. Orienter la puissance d'investissement public, mixée à des capacités d'investissement privé, sur ces sujets serait le bon moyen de permettre à ces écosystèmes de créer leurs marchés, leurs différentiations et *in fine* d'apporter une valeur économique ajoutée en Europe.

Cela nécessite également de faciliter les liens entre la recherche publique et la recherche privée, et de faire en sorte que la recherche débouche sur des projets industriels. Nous devons absolument faire en sorte que tous les acteurs – c'est-à-dire les start-up, les PME, les ETI – soient présents dans ces travaux de recherche. Nous devons aller chercher l'émergence des écosystèmes. L'*Aerospace Valley* en Midi-Pyrénées incarne la rencontre entre le public et les différentes structures privées. Cela crée, au fil du temps, des solutions différenciantes qui vont trouver leur marché et pouvoir se développer.

Il importe aussi, à notre sens, que ces initiatives soient coordonnées au niveau européen. La particularité du numérique est qu'il n'a pas de frontières. Les frontières au sein de l'Europe pourraient donc constituer des freins au développement de ces écosystèmes. Si une entreprise doit s'adapter à une réglementation différente dans chacun des 27 pays, elle peinera à trouver un espace assez large pour se développer. Le Règlement européen sur la libre circulation des données participe de cette démarche et nous soutenons totalement ce texte.

L'échelon européen nous semble également intéressant pour mobiliser des financements conséquents. Certains sujets d'un plan industriel et technologique européen requerront de très lourds financements. Ainsi, il est éclairant d'étudier les financements accordés dans d'autres régions du globe. Après avoir investi 250 millions de dollars dans le développement d'un ordinateur quantique, les États-Unis ont investi à nouveau 1,2 milliard de dollars sur les cinq prochaines années pour appuyer la capacité de développement de cette technologie. La Chine vient également d'investir près de 240 millions d'euros en la matière. Cela représente de très grands budgets. Nous devons utiliser l'échelon européen afin de définir des axes stratégiques et de dédier nos capacités financières à faire émerger le bon écosystème. Cela nous garantira ainsi d'être présents et d'être souverains dans cette technologie en Europe.

S'agissant de la commande publique, nous constatons que la commande des collectivités territoriales et des administrations est peu ouverte aux start-up, aux PME et aux ETI. Les grands marchés sont souvent contractualisés avec les plus grandes structures, et les petites structures sont, par la suite, sous-traitantes de ces grandes structures. Nous le constatons dans l'activité de nos membres : les plus grandes entreprises de services du numérique « décrochent » les marchés publics, puis contractualisent avec des sous-traitants. Cela n'est pas récent. Les petites structures, dans leur développement, doivent intégrer un facteur d'innovation et un facteur différenciant particuliers. Les grandes structures ont évidemment, elles aussi, une capacité à l'innovation. Mais nous aurions tout intérêt à ce que la commande publique soit plus ouverte aux acteurs de plus petite taille. Parmi nos adhérents, 2 000 entreprises sont des PME ou des entreprises de taille inférieure. Leur ouverture vers les marchés publics est très faible. Cela mériterait d'être corrigé à l'avenir.

M. Philippe Latombe, rapporteur. Quelle en est la raison, selon vous ? Les directeurs des systèmes d'information (DSI) dans les collectivités territoriales et les administrations ne sont-ils pas suffisamment informés ? Ou bien cela s'explique-t-il par le fait que les grandes structures pratiquent l'entrisme ou proposent des solutions intégrées et globales ?

M. Benoît Darde. À mon sens, la principale raison tient au code de la commande publique, qui impose des protocoles d'achats lourds à mettre en place. Puisque les protocoles sont lourds, les administrations et leurs DSI préfèrent sûrement mettre en place un protocole d'achat unique et global sur un large périmètre. Cela oriente forcément leurs choix vers des grands acteurs. Si la capacité d'achat des acteurs publics était moins contrainte par de lourds protocoles, la distribution des flux de la commande publique vers un plus grand nombre d'acteurs serait, à mon sens, largement facilitée.

M. Philippe Latombe, rapporteur. À l'inverse, les petites et moyennes entreprises n'ont-elles pas trop peu l'habitude de se regrouper et de travailler en consortium pour répondre de manière collective et globale à ce type d'appels d'offres ? Cela ne marche-t-il pas dans les deux sens ?

M. Benoît Darde. Cela est un bon point. Je trouverais intéressant que l'on trouve des appels à consortiums dans les appels d'offres, et que les acteurs aient cette capacité à se regrouper dans la préparation de leurs réponses. Mais il est très compliqué de faire en sorte qu'un certain nombre de petites structures réussissent à monter un consortium. Les règles en matière de concurrence imposent qu'il n'est pas possible de se mettre d'accord en amont sur la manière dont les activités du marché seront partagées. Un certain nombre de contraintes pèsent sur les appels d'offres, qui risquent de faire considérer les accords entre les membres du consortium comme des ententes. La réponse en consortium est donc également complexe dans sa mise en œuvre. Le plus simple est ainsi que les acteurs de grande taille répondent à l'appel d'offres, puis recourent à une sous-traitance. Mais cela n'aide pas le développement des plus petites structures, car la prime aux marchés publics revient toujours aux acteurs de grande taille.

M. Philippe Latombe, rapporteur. Je comprends que le consortium n'est pas forcément la solution la plus simple ; l'allotissement l'est bien davantage.

Vous employez, depuis le début de l'audition, le terme d'« écosystème ». Pensez-vous que les start-up et les entreprises du numérique ont aujourd'hui la capacité de discuter entre elles de leurs innovations et de leurs orientations, qu'elles s'entraînent mutuellement pour aller plus loin, pour créer une émulation ? Les écosystèmes accueillent-il des discussions qui permettent une mobilisation globale ? Ou, au contraire, le secteur fonctionne-t-il avec des entreprises indépendantes qui protègent leurs activités individuelles ? En bref, pourrait-on facilement atteindre l'interopérabilité ?

M. Benoît Darde. Tous les éléments sont en place pour atteindre l'interopérabilité. J'en veux pour preuve les initiatives en faveur de la création d'un cyber campus, c'est-à-dire un lieu de vie pour cet écosystème et ses entreprises. Mon entreprise de conseil en cybersécurité fait partie du projet de cyber campus. Nous n'avons aucun problème à partager nos visions sur l'évolution de la cybersécurité. Notre manière de coopérer, notre capacité à amener les bonnes compétences au bon moment et au bon endroit feront la différence. Bien sûr, la concurrence existe entre nos acteurs, mais il y a aussi beaucoup de complémentarité. La cybersécurité n'est pas possible sans les éditeurs de logiciels, sans les acteurs de conseil, sans les entreprises de services du numérique, sans les entreprises de conseil en technologies. Nous avons besoin de tout le monde. Cet écosystème échange beaucoup. Je suis témoin des discussions nourries qui ont lieu au sein de la commission des relations institutionnelles de Syntec Numérique. Tous les acteurs y sont réunis, nous discutons des évolutions réglementaires et nous étudions comment ces évolutions ouvriront des chemins propices pour le développement de l'écosystème numérique. Je ne vois pas d'incompatibilité *a priori*.

Mais il faut initier cette dynamique, et cela n'est pas si simple. L'initiative cyber campus va dans ce sens : elle nous aide à nous rencontrer, à être ensemble et à étudier comment dégager des pistes de développement encore plus pertinentes. Grâce au cyber campus, nous serons plus forts ensemble en France pour nous développer à l'international.

M. Philippe Latombe, rapporteur. Faudrait-il développer le concept du cyber campus à l'échelle européenne ?

M. Benoît Darde. Oui.

M. Philippe Latombe, rapporteur. Pour vous, quelle est la bonne échelle ? Est-ce celle du cyber campus européen ?

M. Benoît Darde. La création du cyber campus est France est une excellente première étape. Je pense qu'il faut avancer par étapes, plutôt que de viser tout de suite trop haut et d'échouer. Nous avons besoin de pragmatisme. Il ne faut pas sous-estimer les barrières linguistiques et culturelles en Europe. Nous nous en rendons compte, dans nos entreprises, dans nos propres développements à l'international. Nous devons faire les choses par étapes. Mais il faut viser la coopération à l'échelle européenne, demain ou après-demain.

M. Philippe Latombe, rapporteur. Souhaitez-vous évoquer un sujet sur lequel nous n'avons pas encore échangé ?

M. Benoît Darde. Oui, je souhaiterais aborder le *Digital Services Act* (*DSA)* et le *Digital Markets Act (DMA)*. Nous considérons que ces règlements européens ambitieux sont très bienvenus. Il est très positif de créer un espace de confiance pour les usagers et de savoir proscrire des contenus illicites. Nous sommes complètement partisans de cette approche. Ces règlements encouragent la concurrence tout en reprenant les éléments clés de la directive sur le e-commerce, comme le pays d'origine et la non-obligation de contrôler tous les contenus par les hébergeurs. Ces principes sont très bien repris de la directive sur le e-commerce, qui a fait ses preuves ces dernières années.

Nous retenons néanmoins quelques sujets d'attention dans la mise au point de ce règlement : par exemple, la description du champ d'application et des critères de classification des différents acteurs. Ces aspects sont encore trop flous à notre sens. La Commission a donc encore un peu de travail à réaliser avant la finalisation de ces règlements, dans quelques mois. Nous sommes attentifs à ces travaux, car certaines définitions sont encore beaucoup trop sujettes à interprétation ou renvoient à d'autres textes, eux-mêmes en cours de révision, ce qui limite la capacité d'application et de contrôle de ces textes. Nous serons également contributeurs et vigilants à la gouvernance du *DSA* et du *DMA*. Cette gouvernance permettra de faire évoluer les critères, et nous devons nous assurer que cette évolution est bien maîtrisée et cohérente. Nous gardons donc quelques points d'attention, mais nous considérons très bienvenu le renforcement de la réglementation.

Je souhaite également aborder la fiscalité et le financement du numérique. Le sujet de la fiscalité du numérique doit être traitée au niveau de l'Organisation de coopération et de développement économiques (OCDE). Il faut porter une solution globale. Nous ne sommes pas partisans des solutions nationales, même si celles-ci peuvent constituer une première étape. Nous ne sommes pas favorables aux solutions nationales car l'existence de fiscalités particulières en France peut constituer une barrière à l'entrée pour nos propres entreprises nationales. Cela peut créer des handicaps compétitifs pour les entreprises françaises.

S'agissant du financement, nous considérons qu'il faut continuer à encourager l'innovation dans le numérique et les technologies. Tous les dispositifs fiscaux existants tels que le statut de jeune entreprise innovante, le crédit d'impôt en faveur de la recherche, le crédit d'impôt en faveur de l'innovation, doivent être stabilisés. Ces dispositifs doivent perdurer. Nous devons également recentrer le crédit d'impôt en faveur de la recherche vers les TPE et les PME. En ce sens, nous proposons de supprimer l'agrément fiscal du crédit d'impôt recherche, qui permet la restitution du crédit d'impôt recherche aux sous-traitants. Un certain nombre d'acteurs innovants du numérique sont sous-traitants de grandes entreprises et restituent leurs droits au crédit d'impôt recherche à leurs clients. Or ce sont bien eux qui innovent. Cela est surtout vrai pour les TPE, les PME voire les ETI. Nous demandons donc que ces petites structures puissent faire leur propre déclaration de crédit d'impôt recherche et obtenir des aides leur permettant de poursuivre leur développement. Ce point d'adaptation nous paraît intéressant. Notre écosystème technologique est aussi animé par les petites structures qui se lancent dans une démarche entrepreneuriale et qui sont génératrices de valeur et d'innovation. Le financement doit donc également leur revenir à elles, en direct.

M. Philippe Latombe, rapporteur. Est-ce une position majoritaire et unanime au sein de Syntec Numérique ?

M. Benoît Darde. C'est la position de Syntec Numérique, et c'est un consensus. Ce débat ne se joue pas entre les entreprises membres de Syntec Numérique. Cette position s'entend vis-à-vis des clients. Les entreprises clientes sont, par exemple, de grandes entreprises de certains secteurs. Elles cherchent la restitution du crédit d'impôt recherche par leurs sous-traitants qui sont, eux, des acteurs du numérique. Les plus grands acteurs du numérique réussissent à dire non ; les plus petites structures ne peuvent pas dire non.

Mme Amélia Lakrafi. Je suis absolument d'accord avec M. Benoît Darde sur ce sujet. Ma question porte sur les financements européens. Quelques milliards d'euros sont consacrés à l'innovation pour tous les pays européens. Je sais que les entreprises françaises, et surtout les start-up, ont du mal à y accéder car les demandes de financements doivent être rédigées en anglais. Certaines entreprises n'ont pas les moyens de traduire en anglais un dossier de recherche très technique. Est-ce un sujet sur lequel vous avez travaillé et sur lequel vous avez formulé des propositions ? Avez-vous agi pour que les demandes de financements européens puissent être rédigées en français ?

M. Benoît Darde. Je parle sous le contrôle de Philippine Lefèvre et d'Anissa Kemiche. Je n'ai pas connaissance d'une action que Syntec Numérique aurait menée sur le sujet.

Mme Anissa Kemiche, chargée des affaires européennes, Syntec Numérique. En effet. Nous proposons à nos adhérents un service leur permettant d'être tenus informés des financements ouverts aux niveaux européen, nationaux ou parfois régionaux. Nous menons un certain nombre de travaux et de webinaires avec la Commission européenne, Bpifrance et nos différentes délégations régionales au niveau local.

M. Benoît Darde. Le comité international de Syntec Numérique organise des partages d'expériences en matière de développement des entreprises du numérique en Europe. Un certain nombre d'entreprises viennent témoigner des difficultés qu'elles ont rencontrées et des choix qu'elles ont opérés dans leur développement. En revanche, je ne pense pas que nous ayons mené une action directe sur le point particulier de la constitution des dossiers de demande de financements.

Mme Amélia Lakrafi. Je plaide pour que nos start-up puissent monter des dossiers en français. L'Europe dispose d'un des plus grands systèmes de traduction du monde. L'Union européenne traduit tout. Pourquoi imposer à une start-up de traduire son dossier en anglais ?

M. Benoît Darde. C'est un point qui me paraît plein de bon sens, en effet.

M. Philippe Latombe, rapporteur. Je vous remercie. Si vous souhaitez apporter des compléments à nos échanges du jour, je vous indique que les contributions *a posteriori* seront également prises en compte.

M. Benoît Darde. Nous en prenons bonne note. Nous vous communiquerons également une contribution écrite sur tous les sujets abordés ce jour.

Audition, ouverte à la presse, de M. Nicolas Brien, directeur général de France Digitale
(25 février 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous recevons M. Nicolas Brien, directeur général de France Digitale. France Digitale est la première association de start-up en France. Elle a été fondée en 2012 et réunit désormais plus de 1 800 entrepreneurs et investisseurs, avec l'ambition de soutenir l'émergence de futurs champions européens du numérique.

Nous souhaitons échanger avec vous sur la façon dont les entreprises de l'écosystème du numérique perçoivent la problématique de la souveraineté numérique. Nous sommes évidemment intéressés par votre regard et vos propositions sur la meilleure façon de soutenir le développement de cet écosystème. Nous souhaiterions également aborder le sujet de la numérisation des entreprises françaises, qui constitue un impératif important pour que nos entreprises tirent le meilleur profit de la révolution numérique tout en conservant la maîtrise de leur destin numérique.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

J'aimerais d'abord que vous nous indiquiez ce que recouvre, pour vous, la notion de souveraineté numérique. Ce concept fait l'objet d'une attention croissante de la part des pouvoirs publics, notamment depuis la crise sanitaire. Nous avons, au cours de nos auditions, eu l'occasion de recueillir plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique ou décisionnelle. J'aimerais donc savoir comment, en votre qualité de représentant d'une partie de l'écosystème des entreprises du numérique, vous appréhendez cette notion.

Je souhaiterais ensuite vous entendre sur la situation actuelle des entreprises du numérique. Comment appréhendent-elles cette crise sanitaire qui dure et quelles sont leurs anticipations pour les prochains mois ? J'aimerais également vous interroger sur le niveau de maturité de l'écosystème du numérique français et sur ses attentes vis-à-vis des pouvoirs publics. Quels sont nos forces, nos faiblesses et les leviers d'action prioritaires à mobiliser ? Nos précédentes auditions ont fait apparaître des points clés, comme le rôle de la commande publique, en particulier à destination des petites et moyennes entreprises (PME). Je souhaiterais savoir si vous identifiez d'autres points sensibles et prendre connaissance de vos propositions pour accélérer le développement des entreprises du numérique, dans les prochaines années.

Enfin, je souhaiterais vous entendre sur les différents projets à l'œuvre au niveau européen dans le domaine du numérique, notamment avec le *Digital Services Act (DSA)* ou le *Digital Markets Act (DMA)*. Ces projets vous paraissent-ils adaptés aux défis que nous devrons affronter ces prochaines années ? Avez-vous des attentes ou des points d'alerte spécifiques sur ces textes, que vous souhaiteriez partager avec nous ?

M. Nicolas Brien, directeur général de France Digitale. La souveraineté, pour nous, est assez simple : elle consiste à avoir le choix. Une personne est souveraine quand elle a le choix.

En entrant dans le détail, j'identifie un piège, qui dépend du point de vue auquel on se place pour aborder la notion de souveraineté. Parle-t-on de la souveraineté nationale ou bien de la souveraineté populaire ? J'entends par souveraineté populaire l'idée selon laquelle chaque citoyen est en capacité de faire des choix face aux grandes orientations technologiques que la révolution numérique induit dans son quotidien. Je prendrai un exemple simple : la 5G. Les citoyens ont-ils le choix, ou du moins, ont-ils l'impression d'avoir le choix sur ces questions ? Cela est très important car le numérique est une vague technologique et elle n'est pas anodine. Elle influence notre conception de la démocratie. Nous le verrons lors de la prochaine campagne présidentielle de 2022 : le débat public a lieu de manière croissante dans le champ numérique et à travers des plateformes.

J'attire l'attention sur la souveraineté populaire en ayant recours à une référence historique. Gutenberg a inventé la presse au XV^{ème} siècle et a, de cette manière, commencé à démocratiser le livre. Jules Ferry a rendu l'instruction laïque obligatoire à la fin du XIX^{ème} siècle et a, de cette manière, démocratisé notre capacité à lire. Nous sommes exactement face au même sujet avec le numérique aujourd'hui : nous inventons des solutions numériques absolument remarquables, notamment en intelligence artificielle, mais avons-nous vraiment démocratisé la capacité des citoyens à comprendre ces solutions technologiques ? Je schématiserai de la façon suivante : en matière de numérique, nous avons connu la révolution de Gutenberg, mais nous ne connaissons pas encore la révolution de Jules Ferry. Cela pose problème du point de vue de la souveraineté populaire.

J'explorerai maintenant la problématique de la souveraineté nationale. Nous sommes confrontés à un enjeu intrigant, et pourtant pas très neuf. Avec l'émergence des géants technologiques, notamment américains, les États n'ont plus le monopole des attributs régaliens de la souveraineté comme le cadastre, le fait de battre monnaie, le monopole de la violence physique légitime, l'état civil. Il est de notoriété publique que le fisc grec préfère aujourd'hui utiliser Google Maps plutôt que son propre cadastre. Il est de notoriété publique que Facebook détient davantage de photos d'identité de chacun d'entre nous que n'importe quel service de renseignement. Sur le continent africain, l'on préfère aujourd'hui utiliser Libra plutôt que n'importe quelle autre monnaie émise par un État. Enfin, dans le cadre de la protection de la campagne électorale américaine, il est de notoriété publique que Microsoft a mené l'équivalent de cyberattaques préventives sur des acteurs étatiques russes, iraniens et nord-coréens notamment. Les acteurs privés se dotent aujourd'hui d'attributs régaliens et sont tout à fait capables de se substituer à la souveraineté nationale.

Cela n'est pas nouveau. J'aime à dire que l'on vit un moment « Compagnie des Indes orientales ». Des acteurs privés se sont, par le passé, dotés d'attributs régaliens : cela a soit très bien, soit très mal fini. Que faire face à ces compagnies des Indes numériques ? Je suis d'avis que Mark Zuckerberg finira soit président des États-Unis, soit en prison.

J'en viendrai aux préoccupations concrètes. Plusieurs problématiques liées à la souveraineté ont été posées récemment, notamment du fait des confinements et du COVID. Nous venons de vivre, du fait des confinements, des moments d'accélération digitale sans précédents dans l'histoire de l'humanité. Ces moments d'accélération ont permis de réaliser que le roi était nu. Nous connaissons tous des exemples de décrochage scolaire en raison de la fracture numérique, d'institutions de santé qui n'ont pas pu partager les données car elles n'étaient pas équipées pour le faire, de cyberattaques contre des collectivités locales, de commerçants qui ont basculé dans le digital sans y être préparé, ou d'administrations qui n'étaient pas prêtes au télétravail.

Que fait-on maintenant ? Depuis plusieurs mois, nous nous sommes équipés avec des solutions américaines, ce qui pose problème. Nous ne l'avons d'ailleurs pas tellement fait par

choix, mais plutôt par paresse. Nous avons constaté qu'un processus grave était à l'œuvre : le désarmement technologique de l'État. L'État, les administrations, la haute fonction publique sont aujourd'hui extrêmement démunis d'un point de vue technologique. Le dernier rapport annuel de la Cour des comptes le montre très bien : des monographies sur Pôle Emploi, l'Éducation nationale et Bercy mettent en valeur la perte grave d'expertises technologiques au sein de ces administrations. Cela a un effet pervers, car cela conduit à l'externalisation de l'apport d'expertises technologiques, notamment *via* des contrats. Sur les 450 millions d'euros de contrats pour des prestations de conseil passés par l'État, l'immense majorité concerne des cabinets de conseil technologique. Cela se traduit de la manière suivante : dans les administrations, les personnes ne savent plus expertiser des solutions technologiques et se contentent de passer des contrats avec des intégrateurs (Capgemini, Sopra Steria, Onepoint). Cela peut donner l'illusion, comme ces intégrateurs sont français, que l'on achète français. Cela n'est pas du tout le cas : ces entreprises intègrent des solutions qu'ils ne produisent pas eux-mêmes et qui sont souvent des solutions sur étagère américaines. Devoteam, par exemple, est le premier intégrateur de solutions Google en France. Tout cela est dramatique. Puisque les ministères manquent d'expertises technologiques, personne n'est capable d'expertiser des solutions de start-up françaises ou européennes et de travailler à monter des consortiums et des assemblages technologiques qui pourraient permettre de résoudre un certain nombre de problèmes.

S'agissant des réglementations européennes, j'attire l'attention sur le fait qu'il ne faut pas construire de lignes Maginot numériques. Vous connaissez sûrement la plaisanterie suivante : « Les Américains innovent, les Chinois copient, les Européens régulent ». Nous ne devons pas nous contenter d'une approche défensive. Cette approche est nécessaire : nous devons rééquilibrer nos relations commerciales avec un certain nombre de géants technologiques, notamment américains et chinois. En revanche, nous avons besoin de nos deux jambes pour avancer : la jambe offensive et la jambe défensive.

Je mettrai cela en lien avec la question de la souveraineté populaire. Nous avons aujourd'hui un gros problème d'éducation et de formation : « science sans conscience n'est que ruine de l'âme ». Je vous invite collectivement à relire le rapport Villani à ce sujet, qui esquissait quelques pistes intéressantes, notamment sur l'enseignement des mathématiques et de l'algorithmique. Les élèves ne devraient pas quitter le système éducatif français sans savoir ce qu'est exactement le *smartphone* qu'ils tiennent dans la main toute la journée. En matière de souveraineté populaire, cela devrait être un objectif central de nos politiques afin de réarmer le citoyen.

S'agissant de la formation, la France forme les meilleurs, mais elle en forme peu. Il est très bon d'avoir des médailles Fields, des Prix Nobel, mais il ne peut pas y avoir que des ingénieurs du code. Nous avons également besoin d'ouvriers du code : il s'agit de tous ces métiers qui sont aujourd'hui délocalisés vers la Tunisie, l'Inde, la Roumanie car nous sommes confrontés à une pénurie terrible des métiers du numérique. Les quelques écoles formant ces ouvriers du code en France – Simplon, Epitech, école 42 – ne sont le fruit que d'initiatives privées. Il n'existe pas d'initiative publique en la matière. La Grande école du numérique existe certes, mais elle est arrivée trop tard. En ce sens, il me paraît essentiel de redonner ses lettres de noblesse au terme de « technologie » dans les instituts universitaires de technologie (IUT). L'apprentissage des compétences numériques est extrêmement faible dans les IUT. Cela devrait pourtant être le canal de formation de nos ouvriers du code.

La commande publique est également fondamentale. Nous nous situons à un tournant en la matière : le plan de relance européen de 750 milliards d'euros prévoit d'allouer 20% de son budget, soit 150 milliards d'euros, à la transformation numérique. Il serait dommage que

ces 150 milliards d'euros, plutôt que de dynamiser notre écosystème de start-up européen, aillent gonfler le cours boursier des Google, Apple, Facebook, Amazon et Microsoft (GAFAM). France Digitale milite ardemment pour un *Buy European Technology Act* (BETA) : nous devons établir une forme de préférence européenne, ou de préférence start-up, dans la commande publique. Partout ailleurs dans le monde, il existe un lien extrêmement fort entre la commande publique et les écosystèmes d'innovation. La commande publique y est utilisée comme un levier pour développer les start-up. Nous, Européens, sommes les seuls à ne pas le faire. Cela est assez dramatique.

La loi d'accélération et simplification de l'action publique (ASAP) constitue une initiative intéressante en France. Un de ses articles prévoit de réserver une part de chaque marché public aux PME et aux artisans. Les start-up appartiennent aux PME. Il serait donc ainsi possible de flécher une part des achats publics innovants vers les écosystèmes des start-up. Cela constitue une forme de protectionnisme déguisé : il y a peu de chance pour que les start-up américaines ou malaisiennes étudient les notices de marchés publics en Europe, et ainsi ce seront vraisemblablement les start-up françaises, allemandes ou italiennes qui y répondront.

Pour conclure, il me paraît essentiel de ne pas nous enfermer seulement dans une approche défensive de régulation de l'existant. Nous devons être capables de nous développer grâce à une approche offensive et prospective, qui nous permettra de faire émerger des champions européens.

Je ferai enfin le lien avec la question de la souveraineté nationale et des attributs régaliens grâce à une métaphore historique. Si tout le monde a en tête que la Révolution française de 1789 a entraîné un changement de régime politique, peu de gens ont à l'esprit que la Révolution française a également engendré un changement de normes technologiques. Nous avons évolué des systèmes monarchistes de l'once et du pied vers le mètre et le kilogramme, des systèmes inventés par les Encyclopédistes. Dès lors, la France passera des décennies à exporter son modèle politique et ses normes technologiques, à savoir le système métrique et le kilogramme. Cela a permis à notre pays de dominer la scène scientifique internationale pendant des décennies. Aujourd'hui, les normes technologiques et scientifiques internationales sont imposées par des acteurs non étatiques américains et chinois. Si nous voulons projeter notre propre système de valeurs, nous devons être en mesure de disposer d'acteurs européens en mesure d'exporter des normes scientifiques et technologiques internationales. Cet enjeu est au cœur de la création de champions technologiques européens. Il n'est pas seulement question de créer des emplois et de réussir des levées de fonds à plusieurs centaines de millions d'euros. La question est bien plutôt de savoir si notre continent dispose d'acteurs non étatiques capables de créer et de projeter des normes scientifiques et technologiques internationales. Les normes internationales ne sont pas neutres. Elles sont toujours enracinées dans des systèmes de valeurs. L'émergence des champions technologiques européens est au cœur de l'enjeu d'exportation de normes scientifiques internationales, et cette question doit être prise très au sérieux par nos décideurs.

M. Philippe Latombe, rapporteur. Comment vont les entreprises du numérique depuis la crise et quelles sont vos perspectives à leur sujet ?

M. Nicolas Brien. Je commencerai par évoquer le grand bond en avant digital. Nous avons beaucoup parlé, lors des confinements, de distanciation sociale. En réalité, nous avons connu une distanciation physique mais la plupart de nos interactions sociales ont basculé dans la sphère numérique. Cela a engendré une vaste accélération des usages numériques au niveau mondial. La moyenne d'âge pour l'achat sur les sites de e-commerce, par exemple, a augmenté de dix à quinze ans. Nous sommes donc indéniablement face à un grand bond en avant digital.

À qui profite donc ce grand bond en avant digital ? J'ose penser, d'abord, qu'il profite aux utilisateurs. Il y a toutes les raisons de penser que ces usages ne disparaîtront pas après le COVID. Nous allons subir une intensification des événements climatiques extrêmes du fait du changement climatique. Nous serons donc demain peut-être confinés en raison des feux de forêts ou des tempêtes de neige. Les nouveaux usages numériques développés pendant le confinement sont donc appelés à durer, voire à s'intensifier tout au long du XXI^{ème} siècle.

Comment réagit l'écosystème du numérique face à cela ? Les Américains vont bien, voire très bien : nous nous sommes tous équipés en urgence avec des solutions sur étagère et déjà à l'échelle, c'est-à-dire avec les solutions des GAFAM. L'écosystème des start-up, en revanche, réagit différemment. La crise est très injuste : une start-up opérant dans l'événementiel, le tourisme ou la restauration, sera en échec ; une start-up dans le *cloud* s'en sortira bien mieux. Il ne suffit donc pas d'être actif dans le numérique : il faut avoir déployé des usages numériques dans des secteurs dont les activités ont connu une accélération.

Enfin, le numérique ne se développe pas seulement dans les start-up : il concerne également les grands groupes et les administrations. Nous avons, je l'ai dit, observé en la matière que le roi était nu. Certains grands groupes du CAC40 se sont retrouvés incapables de paramétrer un réseau privé virtuel (VPN) ou d'équiper leurs collaborateurs pour le télétravail.

M. Pierre-Alain Raphan. Je reviendrai tout d'abord sur la formation et sur l'enjeu de l'acculturation aux enjeux du numérique dès le plus jeune âge. Ces aspects constituent, à mon sens, une priorité. La loi a proposé de mettre en place un permis Internet pour sensibiliser les jeunes à ces sujets. Est-il possible d'aller encore plus loin ?

Nous avons soumis hier une tribune proposant de créer des écoles du numérique dans chaque quartier prioritaire de la politique de la ville. À Grigny, dans ma circonscription, le taux de chômage s'élève à 45% chez les 15-25 ans, alors que 100 000 emplois ne sont pas pourvus dans le secteur du numérique. Nous aimerions, peut-être avec votre soutien, que les écoles comme l'école 42 et Simplon puissent ouvrir le champ des possibles pour tous.

Je souhaite par ailleurs évoquer la commande publique. Comment faire en sorte que l'État soit exemplaire dans le soutien à nos pépites ? Le gouvernement prépare une feuille de route à ce sujet. J'aimerais connaître ta vision, Nicolas, au sujet de la commande publique.

J'aborderai enfin la régulation. Nous savons que les textes du *DSA* et du *DMA* sont en préparation. Souhaites-tu relayer des propositions à ce sujet ? Peut-on proposer des régulations de l'économie de l'attention, par exemple ? S'agissant du paiement en ligne, nous savons que certains acteurs sont en abus de position dominante et empêchent l'émergence de start-up françaises. Est-il possible de discuter avec ces acteurs et ces oligopoles ? Comment nous, représentants de la nation, pouvons-nous vous aider à ce sujet ?

M. Nicolas Brien. J'ai lu avec attention votre tribune sur l'éducation. Les jeunes des quartiers populaires sont nombreux à aller en IUT ou en lycées technologiques. Le problème est que ces structures n'ont de « technologique » que le nom. Les écoles du numérique sont peut-être déjà présentes dans chaque quartier sous la forme des IUT et des lycées technologiques. Ne devrions-nous pas former nos ouvriers du code dans ces structures ? Les métiers du numérique sont en tension et cela est vraiment dommage. Du point de vue de la souveraineté nationale, cela implique que nous délocalisons ces métiers à l'étranger. Du point de la souveraineté populaire, il est essentiel de réarmer les citoyens, y compris les catégories populaires. En ce sens, l'une des décisions les plus stupides récemment prises par l'Éducation nationale a été, selon moi, l'interdiction des *smartphones* à l'école. Ne faut-il pas apprendre

aux jeunes à s'en servir, à les dompter, à en avoir un usage éclairé, plutôt que de faire comme si cet objet n'existait pas ?

S'agissant de la commande publique, nous avons observé à la fois un problème de compétences et un problème de conscience. Jusqu'à récemment, très peu de décideurs publics comprenaient l'intérêt des questions de souveraineté numérique. France Digitale a monté le programme France Digitale Campus pour conscientiser les décideurs publics sur ce sujet. Je souhaitais créer un institut des hautes études en souveraineté numérique (IHESN), à l'instar de l'institut des hautes études de défense nationale (IHEDN). L'IHEDN avait été créé par le général de Gaulle pour créer un consensus national parmi les élites autour du programme nucléaire français. Il me désole aujourd'hui qu'aucune structure n'existe pour créer du consensus autour des questions de souveraineté technologique. L'IHESN permettrait de faire émerger du consensus et cela est très important. La France est le seul pays dans lequel le terme de *start-up nation* est politisé ; il fait l'objet de clivages et de débats. Aux États-Unis, en Israël ou en Corée du Sud, personne ne remettrait en cause une forme de consensus technologique. La formation des catégories populaires et la formation des élites sont donc toutes deux importantes.

Il est très compliqué de passer un marché public quand les start-up et les intégrateurs n'ont pas d'interlocuteur compétent et formé au ministère. Qui plus est, les marchés publics de très grande taille excluent de fait les petites entreprises. Si l'on souhaite que la commande publique s'adresse aux start-up françaises et européennes, il faut procéder à de l'allotissement. Mais cela demande une expertise technologique très conséquente au niveau de l'État pour ensuite assembler les « briques ». Personne au sein de l'État, aujourd'hui, ne sait assembler ces briques technologiques. Comme le montre le rapport de la Cour des comptes, il y a trop peu de polytechniciens ou de *data scientists* dans les administrations centrales. Nous constatons donc un désarmement de l'État, qui s'en remet aux grands intégrateurs français qui lui fournissent des solutions américaines intégrées. Le cas du Health Data Hub l'illustre bien : les Américains sont entrés dans le projet par le biais d'un intégrateur français qui était titulaire d'un contrat avec l'Union des groupements d'achats publics (UGAP).

La commande publique pose donc à la fois une question de conscience – qui peut être résolue par la création d'un IHESN – et une question de compétence – qui suppose le recrutement d'expertises technologiques au sein de l'État pour permettre l'allotissement des marchés publics et la bonne utilisation des outils légaux en place. La loi ASAP en vigueur permet d'établir qu'un certain pourcentage des marchés publics innovants revient aux PME. Si cette clause était appliquée, cela serait absolument fabuleux.

Au niveau européen, nous travaillons à pousser un *Buy European Technology Act*, mais nous nous heurtons au sacrosaint droit de la concurrence et à la question des aides d'État. La Commission européenne considère que le fait de privilégier les start-up ou les acteurs communautaires va à l'encontre des traités. Mais un aggiornamento est en cours s'agissant du droit de la concurrence, en raison du COVID. Nous espérons ainsi faire aboutir un certain nombre de nos demandes avant la fin du mandat d'Ursula von der Leyen. Mais nous n'avons pas vraiment le temps d'attendre, car le plan de relance va se déployer dans les dix-huit prochains mois.

Nous sommes favorables au *DSA* et au *DMA*. Ces textes donnent des outils pour rééquilibrer les relations commerciales entre les petits acteurs du numérique et les géants technologiques. Apple, par exemple, produit environ 50% des *smartphones* et commercialise également les applications mobiles à travers son App Store. L'entreprise adopte des pratiques commerciales extrêmement rugueuses, comme l'obligation de passer par son propre système

de paiement. Le *DMA* permettrait de rééquilibrer cette situation en mettant en concurrence différents systèmes de paiement au sein de l'App Store.

Ces textes vont dans le bon sens, néanmoins ils ne doivent pas nous exonérer d'une approche offensive et prospective. Celle-ci passe par l'éducation, la formation et l'orientation de la commande publique vers les start-up. Cela est absolument prioritaire. Cette approche a fait le succès de la Corée du Sud, d'Israël et des États-Unis. Les États-Unis disposent d'un copieux droit de la concurrence, mais ils ont surtout adopté une approche extrêmement offensive : celle-ci s'incarne dans l'agence pour les projets de recherche avancée de défense *(DARPA)*, l'orientation de la commande publique, la présence d'un *chief digital officer* (*CDO)* dans chacune des administrations américaines.

Nous avons deux options pour que l'État reprenne le contrôle sur son expertise technologique. Soit l'on recrée cette expertise technologique en nommant un *chief digital officer* dans chaque administration et ministère – ils formeront un réseau qui permettra de pousser la transformation digitale de l'État de manière offensive. Soit l'on crée enfin une direction générale du numérique qui regrouperait la French Tech, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), certaines compétences du Conseil national du numérique et de l'Autorité de régulation des communications électroniques et des postes (ARCEP) ainsi que toutes les directions des systèmes d'information (DSI) de l'État. Cette direction générale serait confiée au ministre du numérique, qui aurait enfin du pouvoir car il disposerait alors d'une administration conséquente.

M. Philippe Latombe, rapporteur. Ce point est important. Nous avons reçu en audition la direction interministérielle du numérique (DINUM). La DINUM n'est-elle pas cette direction centrale du numérique ? Que devrait-elle alors être ?

M. Nicolas Brien. Non, la DINUM n'est absolument pas cela. Aujourd'hui, l'expertise technologique est faible et éclatée. La DINUM n'est pas capable de donner des instructions au DSI du ministère de la santé, par exemple. Dans ce cas de figure, le DSI s'en remettrait directement au ministre de la santé.

Soit on décide que chaque ministère mène sérieusement sa propre transformation digitale, et on nomme alors un *chief digital officer* dans chaque ministère ; soit la DINUM devient une administration aussi prestigieuse et puissante que la direction générale du Trésor, et on la dote alors des moyens nécessaires en recentralisant un certain nombre de compétences aujourd'hui éparpillées.

M. Philippe Latombe, rapporteur. Vous avez évoqué le problème des compétences au sein des ministères. Pensez-vous que nous disposions actuellement des compétences suffisantes pour monter ce projet de direction générale du numérique, ou devrions-nous nécessairement les recruter à l'extérieur ?

M. Nicolas Brien. Non, nous ne disposons actuellement pas des compétences nécessaires. L'application TousAntiCovid montre bien que l'État ne sait pas fabriquer de solutions technologiques. Cet enjeu est passionnant et se pose souvent aux entreprises qui souhaitent réaliser leur transformation digitale : elles ont le choix entre *buy* (acheter) et *make* (fabriquer). Aujourd'hui, l'État ne sait pas fabriquer et il achète mal. L'on comprend alors aisément que rééquilibrer les rapports commerciaux avec les GAFAM prenne du temps. L'État se rattrape sur d'autres choses, comme la régulation. Je suis d'accord avec cette approche, mais elle ne suffira pas.

M. Philippe Latombe, rapporteur. Que pensez-vous de l'arrêt *Schrems* II ? Déclenche-t-il un séisme, ouvre-t-il une nouvelle ère, ou représente-t-il au contraire un épiphénomène ?

M. Nicolas Brien. On ne peut pas mettre un tigre et un chaton dans une cage et espérer un combat égal. Cela n'est pas spécifique au numérique, mais la relation transatlantique est plutôt déséquilibrée. Je n'attendrais pas grand-chose d'une négociation avec les Américains, d'autant que l'affaire Snowden avait, elle aussi, eu lieu sous l'administration démocrate. Il ne faut pas être naïf : les Américains ont une conscience extrêmement claire de leurs intérêts, et ces intérêts ne sont pas les nôtres.

S'agissant de *Schrems*, la question qui se pose est la suivante : souhaitons-nous faire du protectionnisme numérique ou souhaitons-nous rééquilibrer les forces de marché dans une économie ouverte ? Pour l'instant, il me semble que l'approche adoptée est celle du rééquilibrage des forces de marché dans une économie ouverte : c'est le sens du *DSA* et du *DMA*, du droit de la concurrence ainsi que du *Privacy shield*. Peut-on aller plus loin ? Il me semble que nous glisserions alors dans des considérations dangereuses, comme des impératifs de localisation de la donnée. Je ne suis pas très à l'aise avec cela, ne serait-ce que pour des raisons techniques : il est toujours bon de diversifier ses hébergements, et donc, d'avoir recours à plusieurs serveurs sur plusieurs continents. Je n'ai pas d'opinion tranchée dans ce débat.

La question de l'autonomie stratégique se pose néanmoins dans le registre numérique pour une raison simple : Edward Snowden. Depuis l'affaire Snowden, nous devons arrêter d'être naïfs.

M. Philippe Latombe, rapporteur. Vous avez évoqué, dans votre propos liminaire, le besoin de construire des normes scientifiques et technologiques. L'Europe peut-elle participer à la construction de normes internationales à partir des valeurs qu'elle a développées, notamment s'agissant de la protection des données ? La protection des données constitue-t-elle un critère discriminant, de nature à créer des normes qui feront date ?

M. Nicolas Brien. Fareed Zakaria a publié un essai à la suite de la crise financière de 2008. Il y explique que le XXI^{ème} siècle sera le siècle des trois empires : américain, chinois et européen. Il avance que la seule manière pour l'empire européen de projeter sa puissance sera le droit. Les Européens ont cette capacité à se mettre d'accord à vingt-sept, puis à projeter sur le monde des normes qui ont déjà fait l'objet d'une forme de consensus. Je constate que c'est exactement ce qui s'est passé avec le Règlement général sur la protection des données (RGPD) : l'empire européen, car il est arrivé à un point de consensus à ce sujet, a exporté ses normes et ses valeurs à travers le droit. Nous n'allons évidemment pas exporter le RGPD en Chine, mais le Règlement a fait quelques incursions en Californie, et des pays tels que le Japon et le Brésil se sont alignés sur ce texte. Il s'agit de la projection de la puissance européenne à travers le droit, et en particulier le droit du numérique.

Nous essayons actuellement d'aligner un certain nombre d'États sur nos préoccupations environnementales à travers les accords de libre-échange. Nous devons également être en capacité d'aligner un certain nombre d'États sur nos préoccupations numériques et nos standards en matière de souveraineté numérique à travers les accords de libre-échange. C'est ce qui s'est passé lors des négociations de l'accord entre l'Union européenne et le Japon : le mandat des négociateurs mentionnait clairement le besoin de faire adopter le RGPD par le Japon. Cela constitue, à mon sens, une belle et habile manœuvre de souveraineté européenne : si le cadre normatif qui s'applique au marché japonais est semblable

au cadre normatif européen, les sociétés européennes sont en capacité d'exporter leurs solutions technologiques à moindre coût.

Le droit constitue, selon moi, une approche assez défensive. Mais l'on peut, à travers les accords de libre-échange par exemple – et à la condition d'en confier le mandat à nos négociateurs –, en faire des instruments très offensifs.

M. Philippe Latombe, rapporteur. Je souhaiterais vous interroger sur la fiscalité. Nous sommes confrontés à la fois au problème européen de la fiscalité, qui s'incarne notamment dans la situation de l'Irlande, et au problème des taxes sur les GAFAM, que les pays souhaitent imposer à l'échelon national, à défaut de pouvoir le faire au niveau de l'Organisation de coopération et de développement économiques (OCDE). Quelle vision portez-vous sur les enjeux fiscaux ? Ils constituent, par bien des aspects, le nerf de la guerre en matière numérique.

M. Nicolas Brien. Je suis extrêmement mal à l'aise avec ce débat. Il n'existe pas, à mon sens, d'activités numériques. Le *data center* de Lafarge appartient-il à la catégorie des activités numériques ou du ciment ? Apple est-il un fabricant de *hardware* ou un géant du numérique ? Que devons-nous taxer ? La même question se pose avec Uber et les travailleurs indépendants des plateformes.

Le numérique remet souvent au jour des débats très anciens. J'ai conclu mes études à Colombia University par la rédaction d'un mémoire sur la quantification des flux financiers illégaux. Je m'étais alors intéressé au cas de Starbucks. Les mécanismes d'évitement fiscal mis en place par les géants du numérique sont anciens. Ils ont, pour la plupart, été inventés par Starbucks et McDonald's, dont les activités n'appartiennent pas au champ du numérique. Nous redécouvrons donc aujourd'hui les sujets d'évasion et d'évitement fiscaux sous l'angle du numérique, alors que ces sujets existent depuis bien longtemps. Il en est de même au sujet des travailleurs indépendants pauvres, que nous redécouvrons aujourd'hui sous l'angle de Uber. Je suis mal à l'aise à l'idée de participer à ces débats sous l'angle du numérique, car je crois que ces problématiques sont beaucoup plus larges que le monde du numérique. En mentionnant l'Irlande, vous soulevez la question de la taxation des multinationales. À mes yeux, Starbucks et Apple sont donc exactement dans la même situation.

M. Philippe Latombe, rapporteur. Que pensez-vous de la taxation sur l'activité ? Habituellement, les entreprises sont taxées sur leurs résultats. La taxation sur l'activité implique un changement de paradigme.

M. Nicolas Brien. Je suis mal à l'aise avec cela. Je trouve étrange l'idée de taxer les entreprises sur leur chiffre d'affaires plutôt que sur leurs bénéfices.

M. Philippe Latombe, rapporteur. Cette vision, qui est plutôt une vision européenne, peut-elle poser problème dans nos relations – notamment nos relations concurrentielles – avec les acteurs américains ?

M. Nicolas Brien. Ne vous méprenez pas : je ne suis pas en train d'affirmer qu'il n'est pas besoin de remettre à jour notre corpus fiscal pour épouser les nouveaux produits et services issus du digital. Lors des débats sur la taxe sur les GAFAM, France Digitale a publié une tribune. Nous y mettions en avant l'idée d'une taxe sur la *data* plutôt qu'une taxe sur le chiffre d'affaires. Cette taxe permettrait de faire le lien entre l'utilisation des données personnelles et la production de valeur. Aujourd'hui, les géants technologiques étrangers utilisent cette externalité positive, qui n'est pas taxée. Une telle taxe est difficile à mettre en place car elle suppose de définir le délai et le volume d'utilisation des données personnelles. Nous ne

soutenions pas du tout la taxe sur les GAFAM dans la forme proposée : nous poussions, en revanche, pour l'instauration d'une taxe sur la *data.* Nous nous étions alors fait « taper sur les doigts » par Facebook, qui en avait compris le danger. Je pense qu'il est beaucoup plus habile de taxer la *data* que de taxer le chiffre d'affaires des activités numériques. Il est extrêmement difficile de définir les activités numériques. La première mouture du texte de la taxe sur les GAFAM établissait comme premiers acteurs du numérique en France les groupes Accor et La Poste – il est en effet possible de faire du numérique sans être une start-up et sans produire de solutions digitales.

Évidemment, il serait préférable qu'une telle taxe soit mise en place au niveau européen et international plutôt qu'au niveau national. La technologie n'a pas de frontière, il n'y a pas de raison pour que les régulations technologiques en aient.

M. Philippe Latombe, rapporteur. Y'a-t-il des sujets que nous n'avons pas encore évoqués et sur lesquels vous souhaitez attirer notre attention ?

M. Nicolas Brien. Vous m'aviez interrogé en introduction sur la stratégie européenne en matière de données et sur la cybersécurité. Souhaitez-vous aborder ces enjeux ?

M. Philippe Latombe, rapporteur. Il est vrai que vous avez constaté notre désarmement sur ces sujets. Vous avez affirmé que « le roi était nu ». Pensez-vous que les entreprises françaises sont aujourd'hui suffisamment informées des enjeux du numérique et des risques que celui-ci comporte en matière de protection des données et de sécurité ?

M. Nicolas Brien. Je distinguerai, dans mon propos, les entreprises du CAC40, d'une part, et les TPE et PME, d'autre part.

Les TPE et les PME traditionnelles sont confrontées au sujet de la transformation numérique. Ce sujet n'est pas spécifique à la France, mais il n'a jamais été une priorité des politiques publiques dans notre pays. Les Allemands, eux, ont pris cette question très au sérieux. La France accuse donc aujourd'hui un retard en la matière. Je prendrai pour exemple le dossier de demande d'aides au titre de la transformation digitale des entreprises qu'une commerçante de la région de Nantes m'a fait suivre. Le dossier que les pouvoirs publics demandent aux commerçants de remplir est extrêmement conséquent et détaillé. Qui plus est, ces aides doivent nécessairement couvrir des dépenses supérieures à 5 000 euros – alors que certains commerçants souhaitent seulement créer un site Internet. Cela est problématique, d'autant que l'on sait que la moyenne d'âge des patrons de PME en France se situe autour de 55 ans. La puissance publique prend donc progressivement conscience du besoin de digitalisation des TPE et PME, mais les petites entreprises sont confrontées à des situations folles.

Je suis beaucoup plus dur à l'égard des sociétés du CAC40. Elles ont une responsabilité historique dans le retard de notre pays en matière de numérique. Nous attendons souvent des lobbies qu'ils soient très sévères à l'égard de l'État – France Digitale est également extrêmement sévère à l'égard du CAC40. La situation est affligeante. Je ne comprends pas comment les dirigeants du CAC40 peuvent être aussi peu visionnaires. Ils adoptent des comportements de rentiers et ne voient pas venir les dangers de la transformation numérique pour leur *business model*. Cette situation se traduit par un sous-investissement chronique des entreprises du CAC40 dans le numérique et dans les technologies en général. À titre d'exemple, les débats sur la 5G ont fait rage tout l'été. Quel opérateur de télécommunications français investit aujourd'hui dans les communications quantiques ? Deutsche Telekom et South Korea Telecom sont en train d'investir des millions dans ce sujet et de déployer les premiers réseaux de télécommunications quantiques – alors que nos opérateurs français sont

encore en train de déployer les pylônes 4G. Je constate donc un sujet de sous-investissement chronique dans les nouvelles technologies chez les entreprises du CAC40.

La situation se traduit également par le rachat de start-up. Sans se soucier de nouer des collaborations avec les start-up, les grandes entreprises se contentent de les racheter très cher. J'en veux pour exemple les quelques rachats de start-up à plus de 100 millions d'euros en France : cela est indigent – d'autant que les grandes entreprises n'en font rien.

S'agissant de la cybersécurité, je rappellerai que la France est le deuxième budget de l'Organisation du traité de l'Atlantique Nord (OTAN). Nos grands groupes sont « biberonnés » à la commande publique : Safran, Thales, Dassault Systèmes. Aucune de nos pépites de la cybersécurité ne travaille avec eux ni n'est rachetée par eux. Il n'est pas étonnant alors que les Américains nous dament le pion et que nous ayons du mal à construire une autonomie stratégique.

L'on dit souvent que le poisson pourrit par la tête ; je pense que cela est absolument vrai en matière de transformation digitale de l'économie française. Les réponses devraient se traduire par davantage d'investissements technologiques par les grandes entreprises et surtout par la croissance externe *via* le rachat de pépites technologiques françaises.

M. Philippe Latombe, rapporteur. À quoi cela est-il dû ?

M. Nicolas Brien. Nous en revenons aux compétences. Cela est terrible à dire : les entreprises du CAC40 recrutent des DSI et non des *chief digital officers.* Et quand ceux-ci existent, ils siègent rarement au comité exécutif et ne sont que rarement dotés de budgets importants. Par ailleurs, les *chief financial officers* opèrent les choix financiers stratégiques. Or ces personnes sont peu conscientisées sur les problématiques technologiques.

M. Philippe Latombe, rapporteur. Pourquoi ne le sont-elles pas ? Vous avez dit que les entreprises du CAC40 adoptaient des « comportements de rentiers ». Est-ce à dire qu'elles n'interviennent pas sur les sujets numériques parce que ces investissements coûtent cher et qu'ils les empêchent de verser suffisamment de dividendes à leurs actionnaires ? Ou est-ce uniquement en raison d'un manque total de vision ?

M. Nicolas Brien. Je distingue deux choses. Amazon n'a jamais versé un euro de dividende – et c'est le cas de beaucoup d'entreprises américaines, notamment dans le secteur technologique. Cela s'explique par des raisons culturelles. Les Américains croient que le cours de l'action crée la valeur, et non les dividendes. Il y a vingt ans, Apple était seulement un fabricant de téléphones portables – comme Alcatel ou Nokia. L'entreprise s'est construite progressivement par des acquisitions. Apple n'a pas eu d'idée de génie : elle a racheté des entreprises qui avaient eu des idées de génie – dont l'entreprise française qui a créé la technologie de Siri. L'entreprise est donc progressivement devenue l'entreprise technologique que nous connaissons aujourd'hui. Amazon a connu exactement la même trajectoire : initialement fondée par des libraires, l'entreprise a racheté une start-up de *cloud*, devenue Amazon Web Services. Elle a alors développé une activité de services de *cloud* avec ses serveurs dont la capacité d'utilisation était partielle pendant certaines périodes de l'année. En France, de tels choix stratégiques de croissance externe ne seraient pas acceptés. La priorité se concentre sur la rentabilité envers les actionnaires. Cela constitue une différence culturelle.

M. Philippe Latombe, rapporteur. Si cette différence est culturelle, la situation est-elle la même chez nos voisins allemands ou européens ?

M. Nicolas Brien. Notre rapport annuel sur l'intelligence artificielle a montré que les grands groupes américains investissent six fois plus dans les start-up de l'intelligence artificielle que leurs homologues européens. Cela n'est donc pas seulement un problème français. Nous sommes un vieux continent avec des *legacy players* – cela se traduit culturellement.

Le rachat des entreprises constitue tout de même un sujet particulier en France. Les groupes technologiques français – Atos, STMicroelectronics, Orange – pourraient racheter des start-up, mais ils ne le font pas pour des raisons culturelles et de financement. Il manque un certain nombre d'acteurs financiers pour fluidifier ces transactions. Je souligne, à ce sujet, le rôle des fonds de *tech buy-out* aux États-Unis. Ces fonds sont capables de racheter une première start-up, puis une seconde qui lui est complémentaire, de les fusionner puis de les revendre à un grand groupe. Il existe une cinquantaine de fonds de *tech buy-out* sur Market Street à San Francisco : vous en trouverez péniblement deux en France. Nous pourrions en créer. J'avais suggéré à l'Élysée l'idée que le Fonds européen d'investissement (FEI), qui a aujourd'hui des activités de fonds de fonds dans les domaines de *Venture Capital* ou de *Private Equity*, pourrait conduire des activités de fonds de fonds de *tech buy-out.* Cela permettrait, par exemple, qu'un fonds de *tech buy-out* rachète Blablacar puis Flixbus et les fusionne pour créer un champion européen.

M. Philippe Latombe, rapporteur. Relevez-vous d'autres sujets que notre mission d'information devrait absolument explorer ? Nous avons déjà traité la question des achats et de la commande publique. L'éducation fera l'objet d'un prochain cycle de travaux. Devrions-nous être attentifs à d'autres sujets ?

M. Nicolas Brien. Je pense avoir mentionné les enjeux principaux, en particulier la commande publique et l'éducation et la formation. L'éducation et la formation concernent aussi bien les catégories populaires que les élites. Les élites ont un rôle à jouer. Si vous nous le demandiez, nous transformerions demain notre France Digitale Campus en IHESN.

La question stratégique est essentielle. Jouer défensif est bien, jouer offensif est mieux. Nous avons tout ce qu'il faut pour le faire. Nous devons définir notre vision : quelle est, aujourd'hui, la troisième voie européenne ? Nous devons être capables de projeter une vision positive. Nous ne pouvons pas être simplement la voie alternative à la Chine et aux États-Unis.

France Digitale réfléchit beaucoup à l'entreprenariat technologique à impact. Parmi les start-up à impact environnemental ou social positif, les leaders mondiaux ou européens sont français. Il s'agit de l'application de covoiturage Blablacar, qui permet d'économiser l'équivalent de la production de CO_2 de la ville de Paris ; de Too good to go, qui permet d'éviter le gaspillage alimentaire ; de BackMarket, qui permet de commercialiser des *smartphones* reconditionnés. Je pense que nous tenons quelque chose. En Europe, nous avons à cœur de ne pas innover pour innover, mais d'innover à des fins de progrès social. Nous avons des champions pour porter ce message. À mon sens, ces champions méritent d'être valorisés. À titre d'exemple, le Président de la République a réuni à l'Élysée le Tech for Good Summit : il y a invité le fondateur de Twitter et la Première ministre de Nouvelle-Zélande, mais je n'y ai pas vu beaucoup d'entrepreneurs technologiques à impact français ou européens. L'entreprenariat technologique à impact est une vision intéressante à porter.

M. Philippe Latombe, rapporteur. L'idée est bien prise. Si vous souhaitez apporter des compléments à nos échanges du jour, les contributions *a posteriori* seront également prises en compte.

M. Nicolas Brien. À nos yeux, le seul critère est le critère d'urgence. Le plan de relance va se déployer au cours des dix-huit prochains mois. Les missions d'information et d'enquête sont précieuses, mais elles sont rarement orientées vers une temporalité aussi courte. À mon sens, il faut définir une feuille de route très pratique et très claire en matière de souveraineté technologique dans les dix-huit prochains mois. Nous avons la possibilité de mobiliser des moyens énormes, profitons-en.

M. Philippe Latombe, rapporteur. C'est l'objectif que nous nous sommes fixés.

Audition, ouverte à la presse, de M. le docteur Laurent Treluyer, directeur, Mme Hélène Coulonjou, directrice déléguée auprès du directeur, et Mme Elisa Salamanca, responsable du département Web, Innovation, Données, de la direction des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP)
(4 mars 2021)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos auditions sur la souveraineté numérique et les données de santé. Après avoir échangé avec les représentants du Health Data Hub et du Ouest Data Hub, au mois de février dernier, nous recevons aujourd'hui trois représentants de la direction des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP).

L'AP-HP rassemble 39 hôpitaux qui accueillent chaque année plus de huit millions de patients. Elle agit en faveur de la transformation numérique de notre système de santé au service d'une meilleure prise en charge des patients. L'utilisation du logiciel Orbis, par exemple, facilite la dématérialisation des informations de santé et leur échange entre praticiens. L'AP-HP possède également un entrepôt de données de santé : celui-ci constitue un outil de recherche et d'expérimentation des technologies de pointe, comme l'intelligence artificielle et le *big data*. L'AP-HP est donc directement concernée par les enjeux de protection des données et des systèmes d'informations face aux cyberattaques.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

Je souhaiterais tout d'abord que vous nous présentiez un état des lieux de la politique du numérique de l'AP-HP : nous aimerions disposer d'une vision claire des principales initiatives mises en œuvre dans ce cadre. Notre mission d'information portant sur le thème de la souveraineté numérique, j'aimerais savoir comment vous appréhendez cet enjeu et comment vous l'intégrez à vos choix technologiques. Cela nous permettra d'échanger sur les principaux choix techniques effectués et leurs motivations. Enfin, pour être complet sur la transformation numérique de la santé, je voudrais savoir comment ces évolutions sont perçues par les acteurs de la santé et de quelle façon il est possible de les mobiliser au service de cette politique.

Ma deuxième question concerne la collecte et la gestion des données de santé. Plusieurs initiatives sont à l'œuvre en la matière, et l'une d'entre elles a été fortement médiatisée : le Health Data Hub. En 2019, le directeur de l'AP-HP, M. Martin Hirsch, s'était inquiété de ce que « le Health Data Hub puisse fragiliser l'expertise des centres hospitaliers sur leurs données ». Je voudrais savoir si ces inquiétudes sont levées, d'une part, et, d'autre part, recueillir votre avis sur le recours, par le Health Data Hub, à une solution américaine, le *cloud* Azure de Microsoft, pour héberger les données. Je souhaiterais également vous entendre, en comparaison, sur le fonctionnement concret de l'entrepôt de données de l'AP-HP.

Enfin, l'actualité récente est marquée par des cyberattaques contre les systèmes d'information des établissements de santé. Face à la sophistication de la menace cyber, comment est-il possible, selon vous, de garantir un niveau de protection maximale à nos infrastructures numériques, en particulier dans le domaine de la santé ?

Dr Laurent Treluyer, directeur des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP). L'AP-HP est un établissement universitaire qui couvre Paris et sa petite couronne : il réunit 39 établissements et plus de 100 000 personnels médicaux et non médicaux. Nous avons défini cinq axes pour le développement de nos systèmes d'information – ces axes ont été renforcés en 2015 dans les schémas directeurs pour la période 2015-2020.

Le premier axe consiste à établir un système d'information orienté sur le patient. L'objectif d'Orbis est de permettre à l'ensemble des professionnels de santé de l'AP-HP d'utiliser le même outil et d'accéder au même dossier patient informatisé sur l'ensemble de l'AP-HP. Ce logiciel couvre des fonctions extrêmement larges : le dossier médical, la prescription, les urgences et le dossier social. Nous avons déployé cet outil dans 80% de nos services et au sein de l'ensemble de nos établissements. Ce déploiement a commencé il y a près de dix ans et devrait prendre fin en 2022. Cet outil, maintenant largement déployé au sein de l'AP-HP, permet un meilleur suivi des patients tout au long de leurs parcours. À titre d'exemple, un malade arrivant aux urgences de Lariboisière, transféré à la Pitié Salpêtrière en réanimation, puis admis en soins de suite dans un autre hôpital, dispose du même dossier patient tout au long de son parcours et bénéficie d'un suivi extrêmement précis de ses données médicales. Plus de 10 millions de patients et 80 000 utilisateurs sont aujourd'hui référencés dans Orbis.

Nous avons également informatisé l'ensemble de nos plateaux médico-techniques. Un outil commun à l'ensemble de l'AP-HP permet à tous les radiologues et les cliniciens de consulter les radios, les scanners et les imageries par résonance magnétique (IRM) réalisés dans tous les établissements de l'AP-HP. Nous avons également mis en place un système d'échange avec nos collègues des autres établissements publics et privés, à l'échelle régionale. Nous avons également informatisé l'ensemble des parcours de soins en biologie. Ce travail de refonte est long, et nous menons également un important travail de mutualisation. En médecine nucléaire, par exemple, nous utilisions par le passé quatre logiciels différents : nous avons acquis un seul logiciel pour l'ensemble des douze services de médecine nucléaire de l'AP-HP. Ce travail de refonte, de mutualisation, de consolidation de nos dossiers patients a lieu en continu.

Nous avons également travaillé sur les parcours et les territoires de santé. Nous avons implanté de nouveaux outils comme la messagerie de sécurité de santé, qui permet en particulier de fluidifier les relations avec les médecins traitants. Nous expérimentons et déployons également le dossier médical partagé (DMP), ainsi que des outils régionaux comme Terr-eSanté.

Nous avons également voulu fortement améliorer la relation avec les patients. Pour cela, nous avons mis en place un portail « patient » : 15 000 patients étaient inscrits au 15 janvier 2020, ils sont plus de 160 000 désormais. Grâce à ce portail, les patients peuvent s'inscrire dans nos établissements, préparer leur parcours administratif grâce à la préinscription administrative, prendre rendez-vous, procéder aux règlements de leurs soins ainsi qu'accéder à l'ensemble de leurs comptes rendus et de leurs ordonnances. Ce service a connu une montée en puissance très importante tout au long de l'année 2020. Nous déployons également de nouveaux services sur le portail : il sera prochainement intégré dans l'espace numérique de santé.

Nous avons également refondu toutes nos activités de gestion financière, logistique et patrimoniale. Nous évoluons ainsi vers la dématérialisation des bulletins de paie. La fonction publique hospitalière, contrairement à la fonction publique d'État, n'a pas l'obligation de dématérialiser les fiches de paie. Le directeur général a décidé d'évoluer vers la

dématérialisation. Nous avons également refondu l'ensemble de nos logiciels de facturation : nous utilisions par le passé un seul outil, qui était implanté dans nos 39 hôpitaux. Nous utiliserons désormais un seul outil mutualisé pour l'ensemble de nos hôpitaux et relié à Orbis. Nous avons également investi dans les outils de gestion des ressources humaines.

Nous menons également un travail important sur nos infrastructures, nos systèmes d'information, l'architecture et l'hébergement. Ces travaux sont très conséquents et grandement consommateurs de ressources et de compétences.

Notre dernier axe « recherche » porte sur les systèmes d'information qui aident la recherche. Cet axe représente un investissement important. Le directeur général a ainsi souhaité implanter dès 2015 un entrepôt de données de santé, qui collecte l'ensemble des données de santé de l'AP-HP et les met à disposition des chercheurs. L'AP-HP est également opérateur national pour la banque nationale des données de maladies rares, et opérateur du projet SeqOIA sur la bioinformatique. Elle est également opérateur et maître d'œuvre du système d'information de dépistage populationnel (SIDEP), un des trois grands projets pour le suivi de la crise COVID.

Mme Elisa Salamanca, responsable du département Web, Innovation, Données, de la direction des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP). La création de l'entrepôt de données de santé a été engagée à la fin de l'année 2015. Il se compose de structures organisationnelles et de gouvernance ainsi que d'infrastructures technologiques. Je vous présenterai, pour ma part, les choix technologiques opérés pour développer ces différentes infrastructures.

L'entrepôt de données de santé repose sur la collecte des données, puis sur leur consolidation : il s'agit de leur mise en forme, leur mise en qualité, leur standardisation. Interviennent ensuite les outils mis à disposition pour traiter les données, c'est-à-dire l'infrastructure de calcul.

Nous distinguons en la matière trois grands cas d'usage. Le premier, et le plus connu des cas d'usage, concerne la mise à disposition des données de soins à des fins de recherche ou d'appui à la recherche clinique. Le second cas d'usage concerne le pilotage : il s'agit d'utiliser les données médicales pour piloter l'activité hospitalière. Enfin, le dernier cas d'usage bénéficie à l'innovation : il consiste à réutiliser les données pour faciliter l'innovation numérique, par exemple par le développement d'algorithmes d'intelligence artificielle ou par la création d'interfaces d'accès standardisées aux données de l'AP-HP.

Nous avons choisi l'*open source* pour développer l'entrepôt des données de santé pour des raisons assez diverses. Tout d'abord, aucun outil sur étagère n'était capable de traiter notre projet dans sa globalité. Nous nous sommes donc appuyés sur l'outil i2b2 *(Informations for Integrating Biology & the Bedside)* : ce logiciel permet de créer des cohortes de patients. Il s'agit d'un outil *open source* développé par un hôpital aux États-Unis, qui est aujourd'hui utilisé par environ 250 hôpitaux dans le monde. Le recours à l'*open source* permet de bénéficier d'une très grande communauté. Nous avons souhaité nous insérer dans cette communauté internationale de l'*open source*, pour deux raisons principales : d'une part, aucun outil propriétaire n'était disponible sur le marché pour répondre à l'ensemble de nos besoins ; d'autre part, nous souhaitions maîtriser les outils que nous mettions en place et jouir d'une certaine indépendance. En matière de stockage de bases de données par exemple, nous utilisons PostgreSQL plutôt qu'Oracle. La maîtrise des coûts entre évidemment également en jeu : les solutions *open source* sont parfois moins chères que les solutions propriétaires. Enfin, nous estimions qu'utiliser l'*open source* nous permettait d'atteindre une meilleure capacité d'adaptation et d'être plus agiles dans le déploiement de nos outils.

Comment s'est construit l'entrepôt de données de santé ? La base de données de l'AP-HP contient à ce jour les données de plus de treize millions de patients. Nous avons mis en place la plateforme Jupiter, qui permet aux équipes de recherche de travailler sur les cohortes d'intérêt. Chaque espace de travail dispose des outils de *data science* classiques comme Python et R, et a accès à notre *cluster* de calcul qui est capable de conduire tout type de traitement sur les données : il permet de procéder aussi bien à des biostatistiques classiques qu'à de l'apprentissage automatique grâce à la puissance de calcul mise à disposition.

L'AP-HP a fait le choix, dès 2015, d'opter pour une infrastructure *on-premise* et non en *cloud*. Ce choix répondait à deux considérations : d'une part, la communauté médicale avait exprimé le souhait de maîtriser les données de l'AP-HP ; d'autre part, nous n'avons pas ressenti, jusqu'à présent, le besoin technique de recourir à des infrastructures *cloud* extérieures. La puissance de calcul que nous sommes capables de mettre à disposition de nos équipes de recherche est largement suffisante pour couvrir les besoins des projets en cours. Plus d'une centaine de projets ont été déposés auprès de nos instances et une centaine de projets sont aujourd'hui en cours sur nos infrastructures. La mise à disposition des données à des fins de recherche bénéficie donc d'une *stack* logicielle *open source*.

En revanche, en ce quoi concerne l'utilisation des données de santé pour le pilotage de l'activité hospitalière, nous avons eu recours à un outil existant sur le marché. Il était à la fois plus efficace et moins coûteux de s'appuyer sur cet outil, qui répondait complètement à nos besoins. Nous avons donc choisi une solution propriétaire d'IBM. Nous utilisons cette solution pour produire des indicateurs que nous restituons aux cliniciens, aux cadres de services médicaux, à la direction générale et aux directions des groupes hospitalo-universitaires.

Les choix opérés en matière de solutions technologiques nous laissent donc aujourd'hui la capacité de créer des interfaces entre plusieurs solutions. Par exemple, en matière de services d'information pour la recherche, nous souhaitons créer une boucle de rétroaction, c'est-à-dire alimenter la recherche clinique avec les données de soin et vice-versa. Nous travaillons ainsi à la fois avec des éditeurs de logiciels et avec des solutions *open source*, pour ouvrir un large spectre d'outils à nos chercheurs et couvrir l'intégralité de leurs besoins.

Mme Hélène Coulonjou, directrice déléguée auprès du directeur des systèmes d'information de l'Assistance publique – Hôpitaux de Paris (AP-HP). L'AP-HP a organisé une gouvernance de la donnée, principalement centrée aujourd'hui sur l'entrepôt de données de santé, mais qui a vocation à s'étendre à l'ensemble des données de vie réelle produites au sein de notre centre hospitalier universitaire (CHU). L'entrepôt de données de santé ne couvre en effet qu'une partie des données de santé, car les données qui y sont stockées sont structurées et directement exploitables.

La gouvernance s'organise en trois niveaux. Le niveau de terrain, d'abord, est extrêmement important. Il rassemble, au sein des départements hospitalo-universitaires (DHU), des *data scientists* en poste au sein des unités de recherche clinique. Ces unités sont dirigées par des professeurs d'université et des praticiens hospitaliers qui ont pour mission de piloter la recherche clinique de l'AP-HP. Le niveau de terrain rassemble également des représentants des médecins des départements d'information médicale (DIM) qui interviennent sur le versant pilotage. Ces comités d'utilisateurs font remonter les préoccupations du « terrain », et inversement, diffusent les bonnes pratiques mises en œuvre.

Au cœur de la gouvernance se trouve le comité scientifique et éthique (CSE) de l'entrepôt de données de santé. Il est dirigé par Mme Marie-France Mamzer, professeure d'éthique médicale à l'université de Paris. Il rassemble une trentaine de membres. Il a été refondé il y a moins de deux ans pour être plus représentatif et plus adapté à sa fonction : il

rassemble désormais non seulement des médecins, mais aussi des praticiens de la recherche (chefs de projets ou biostatisticiens par exemple), des personnels paramédicaux, puisqu'ils utilisent aussi bien que les médecins les données de l'entrepôt de données de santé, des représentants des patients et, enfin, des invités extérieurs. Les invités extérieurs n'ont pas de droit de vote mais ils apportent une expertise complémentaire à celle des cliniciens, notamment dans le domaine des mathématiques appliquées. Le CSE réunit ainsi des représentants de l'Institut national de recherche en sciences et technologies du numérique (Inria) ou de l'université de Paris dans ce domaine. Le CSE est ainsi le « cœur du réacteur ». Il a pour mission, dans un certain nombre de cas, de donner accès aux données.

Au sommet de cette gouvernance se trouve un comité de pilotage de la donnée au sein de l'AP-HP. Il est très majoritairement composé de médecins directement intéressés par le sujet, représentants de la commission médicale d'établissement et de ses sous-commissions recherche et numérique. Il est co-présidé par le vice-président « recherche » du directoire de l'AP-HP et par une directrice générale adjointe de l'AP-HP. Ce comité poursuit une vocation décisionnelle : il se réunit chaque trimestre afin de décider des arbitrages et des orientations pour l'ensemble de la politique de la donnée à l'AP-HP.

Comment accède-t-on aux données de l'entrepôt de données de santé ? On distingue quatre cas de figures. Si le périmètre de l'accès souhaité est celui de l'équipe de soins, c'est-à-dire de l'unité fonctionnelle au sein du service, l'accès pour ces personnels est direct et sans formalisme particulier. L'accès se fait *via* les outils et les portails que Mme Elisa Salamanca a décrits précédemment.

Si le périmètre déborde celui de l'équipe de soins, c'est-à-dire qu'il se situe toujours au sein de l'AP-HP mais qu'il va au-delà de l'unité fonctionnelle, ce cas de figure est celui d'une recherche multicentrique. Le porteur du projet de recherche est tenu d'adresser ce projet pour examen et validation au CSE. Ce comité se réunit mensuellement : sa validation est la condition pour qu'un espace sécurisé d'accès aux données, individualisé et propre à la recherche en question, soit ouvert sur le portail Jupiter avec les outils afférents.

Dans le troisième cas de figure, un projet de recherche, quel que soit son périmètre, associe un partenaire extérieur public ou privé. Dans ce cas, notre commission médicale d'établissement a récemment formalisé les règles d'accès aux données. Ce partenariat est possible à la condition que le CSE ait validé le projet, c'est-à-dire suivant la même procédure que dans le deuxième cas de figure.

Enfin, dans le quatrième cas de figure, la demande d'accès concerne les données de l'entrepôt de données de santé de l'AP-HP, en plus des données de santé d'autres établissements de santé. S'applique alors la procédure classique : le porteur de projet doit bénéficier d'une autorisation délivrée par la Commission nationale de l'informatique et des libertés (CNIL) sous réserve d'examen. Ce cas de figure sort du cadre de référence de l'entrepôt de données de santé de l'AP-HP, qui est celui de l'engagement au respect de la méthodologie de référence dite MR-004 de la CNIL, qui permet les trois cas de figure précédents.

Dans tous les cas, la règle est que les données de santé de l'AP-HP ne sortent pas de l'environnement de l'AP-HP. Le cas exceptionnel dans lequel les données en sortiraient est, le cas échéant, soumis à la validation du comité de pilotage. Ce cas s'est présenté une seule fois, il y a deux ans, dans un projet conduit avec l'Inria : les données ont été temporairement exportées, pour des raisons de puissance de calcul, au centre de l'Inria de Sophia Antipolis. Aucun autre cas ne s'est présenté jusqu'à présent.

Je souhaiterais enfin mentionner les productions réalisées à partir de l'usage de ces données. Il faut distinguer les données de l'entrepôt de données de santé de l'ensemble des données massives de l'AP-HP, lesquelles sont aujourd'hui le plus fréquemment utilisées dans de grands projets de recherche et développement. Nous menons ces projets avec des partenaires privés, soit de projets européens, soit de projets nationaux, de type projets structurants pour la compétitivité, comme par exemple l'action de recherche hospitalo-universitaire en santé (RHU) qui est gérée par l'Agence nationale de la recherche (ANR) ou par Bpifrance au titre des investissements d'avenir. Nous pourrons évidemment vous transmettre, si vous le souhaitez, la liste des travaux en cours et des objectifs visés ainsi que la liste des publications d'ores et déjà réalisées à partir des données de l'entrepôt de données de santé.

M. Philippe Latombe, rapporteur. Comment votre entrepôt de données et l'ensemble de votre gouvernance s'inscrivent-ils dans le projet Health Data Hub ?

Dr Laurent Treluyer. Il nous semble important que des centres de données régionaux se créent dans les CHU. Il existe une notion de proximité s'agissant des données. Nous constatons tous la difficulté de mettre ensemble des données d'origines diverses dans un monde peu standardisé et non normalisé. Il est illusoire de rassembler dans un même entrepôt de données de santé, par exemple, l'ensemble des données de biologie et de vouloir en tirer de la valeur. Nous avons donc souhaité mettre en place la proximité avec la donnée et la proximité des outils avec nos chercheurs. Considérant la taille de l'entrepôt de données de santé de l'AP-HP, celui-ci réunit aujourd'hui suffisamment de données pour conduire l'ensemble des recherches qui nous sont demandées. Il est un des plus importants et des plus riches entrepôts de données de santé en ce qui concerne la quantité et la qualité de la donnée.

Nous entretenons des liens forts avec le Health Data Hub, car nous conduisons des projets communs de collaboration. Plusieurs de nos personnels sont financés par le Health Data Hub pour un certain nombre d'études. Nous menons donc une discussion permanente avec lui. Même si notre place est très minoritaire dans sa gouvernance, nous sommes néanmoins membre de son conseil d'administration.

Cette articulation n'est pas toujours simple, mais nous y travaillons de manière importante. Nous nous rencontrons régulièrement et nos équipes nourrissent de nombreux échanges. Nous avons par exemple récemment partagé avec le Health Data Hub nos travaux sur le langage naturel. Il s'agit donc d'un processus de travail permanent. Il est vrai, cependant, que notre communauté médicale nourrit une attention particulière quant au transfert de données médicales vers des tiers. Cela fait partie des sujets sur lesquels le Health Data Hub est extrêmement prudent. Ce sujet fait débat au sein du comité de pilotage, et une attention particulière lui est accordée.

M. Philippe Latombe, rapporteur. Nous avons récemment auditionné les représentants du Ouest Data Hub, hub interrégional qui fonctionne de manière similaire au vôtre, au regard, à la fois, de l'infrastructure technologique et de la gouvernance de la donnée. Le Health Data Hub, lui, adopte une architecture tout à fait différente. Il constitue donc une couche supplémentaire qui s'ajoute à vos infrastructures, avec un *cloud*. Comment les deux structures peuvent-elles se marier de façon efficace ? Est-il possible de garder votre gouvernance et votre structure propres tout en contribuant au Health Data Hub ?

Dr Laurent Treluyer. Je répondrai à votre question en abordant tout d'abord le *cloud*. Nous ne sommes pas opposés au *cloud* : nous sommes très attentifs à ce sujet, et nous réfléchissons aujourd'hui à des solutions de *cloud* souverain. Nous menons ces discussions avec des fournisseurs de *cloud*. Pour le moment, notre infrastructure supporte la charge de nos

besoins en matière de puissance de calcul. Nous savons cependant que nous devrons faire face, à l'avenir, à des demandes de puissance de calcul supplémentaires auxquelles nous ne pourrons répondre. Nous pourrons alors avoir besoin de recourir à des puissances de calcul extérieures, soit *via* des instituts publics comme l'Inria, soit *via* des hébergeurs de *cloud* privés. Il n'y a pas d'opposition au *cloud* de notre part. Nous sommes face à un vrai sujet technique. Nous menons actuellement des projets pilotes, des expérimentations et des collaborations avec différents fournisseurs de *cloud*.

Il est nécessaire de penser l'articulation dans la gouvernance. Nous menons actuellement des discussions sur la valorisation des données et un certain nombre de débats sont en cours. Nous défendons le fait qu'il faut différencier nos études. Dans le cas des études de recherche par exemple, les chercheurs formulent certaines de leurs demandes au niveau de l'AP-HP, mais conduisent également des études nationales, pour lesquelles le Health Data Hub a toute sa place. Nous n'allons pas collecter dans notre entrepôt les données de santé de l'ensemble des CHU de France : c'est le travail du Health Data Hub. Les rôles dépendent donc vraiment du périmètre de recherche. Il faut considérer l'articulation comme une complémentarité et non comme une opposition. Nous avons toujours insisté sur le fait que le Health Data Hub intervenait en complémentarité de nos activités. Un entrepôt de données de santé est composé de plusieurs couches et il est normal qu'il existe des couches régionales. Il est évident que chaque groupement hospitalier de territoire (GHT) ne va pas construire son entrepôt de données de santé, en raison des investissements et des compétences importantes requises. Nous ne sommes donc pas en opposition avec le Health Data Hub : il s'agit de construire une complémentarité entre différentes couches, en fonction des besoins de nos cliniciens et de nos chercheurs.

Les débats qui ont cours actuellement concernent par exemple le point de savoir comment nos entrepôts de données de santé régionaux pourraient facilement accéder au système national des données de santé (SNDS). Nous devons travailler avec eux à ce sujet. Ce sont des sujets techniques, qui posent encore des difficultés. Nous devons trouver les bonnes solutions.

M. Philippe Latombe, rapporteur. Vous avez opéré un choix très marqué d'utilisation des logiciels *open source*, notamment en ce qui concerne l'utilisation des données de santé pour la recherche. Ces choix logiciels sont-ils compatibles avec les choix d'autres CHU ou d'autres hubs régionaux d'utiliser des outils sur étagère ? Ou au contraire, cela va-t-il donner lieu à une convergence vers des outils communs ?

Dr Laurent Treluyer. Il s'agit de vrais choix stratégiques. Je ne crois pas à l'existence d'une solution unique pour l'ensemble du territoire. Il peut y avoir des choix stratégiques différents. Nous devons nous y adapter. Si d'excellents outils étaient mis sur le marché et qu'il était plus simple et moins coûteux de recourir à des logiciels sur étagère, nous le ferions.

Nous avons opéré le choix de l'*open source*, au départ, car nous n'avions pas les outils nécessaires quand nous avons démarré le projet de l'entrepôt de données de santé. En ce qui concerne le pilotage, en revanche, nous avons recouru à des logiciels du marché. Nous opérons donc des choix très pragmatiques. L'*open source* fonctionne bien, nous sommes satisfaits de nos solutions et nos chercheurs le sont aussi. Mais nous n'avons jamais décidé de n'utiliser que de l'*open source* : ces questions pourront se reposer au comité de pilotage si de nouveaux outils efficients et simples émergeaient sur le marché.

Ces expérimentations font partie de l'activité d'un hôpital universitaire comme l'AP-HP, notamment dans nos collaborations avec l'Inria. Nous avons créé un véritable laboratoire

de recherche sur les données, en commun avec l'Inria, qui a été inauguré hier. Il est normal qu'un établissement comme l'AP-HP prenne un peu d'avance sur ce type de sujet.

M. Philippe Latombe, rapporteur. Je vous ai interrogé, dans mon propos liminaire, sur la cybersécurité. Disposer d'une équipe de développeurs en interne, capables d'utiliser et de développer les solutions dont vous avez besoin à partir de logiciels en *open source*, constitue-t-il une force pour la protection et la sécurité de vos données ? Cela vous apporte-t-il une réactivité supplémentaire ? Était-ce aussi une composante des choix stratégiques que vous avez opérés dès le départ ?

Dr Laurent Treluyer. Il s'agit ici davantage de souveraineté que de sécurité. Les grands fournisseurs de *cloud* américains ont une expertise manifeste et importante en matière de cybersécurité. Évidemment, les hackers sont en train d'essayer de s'infiltrer dans le *cloud.* On entend dire que le *cloud* est sécurisé et qu'à l'inverse, les infrastructures *on-premise* ne le sont pas. Tout cela est un peu plus compliqué : il y a en réalité beaucoup plus de valeur dans le *cloud* que dans chaque établissement de soin.

L'*open source* est un choix stratégique de développement. Nous intégrons la cybersécurité dans nos choix de développement le plus en amont possible, selon le principe de *security by design* et de *privacy by design*. Il n'est pas simple de disposer des deux aspects, à la fois la sécurité et la confidentialité, dès le démarrage. Nous nous efforçons de le faire avec le responsable de la sécurité des systèmes d'information (RSSI) et la déléguée à la protection des données (DPO) de l'AP-HP. Les éditeurs ont du mal à incarner cette vision : les audits d'intrusion et de sécurité montrent que les éditeurs ont encore du travail à faire pour se mettre à jour à ce sujet.

M. Philippe Latombe, rapporteur. Vous vous efforcez d'intégrer la partie cybersécurité très en amont, suivant le principe de *security by design*. Comment faites-vous ? Utilisez-vous des solutions ou des expertises déjà existantes, par exemple développées par des start-up ? Travaillez-vous vous-mêmes à la création de solutions de cybersécurité ?

Dr Laurent Treluyer. La partie développement est une faible partie de notre activité. En matière de systèmes d'information, nous développons des solutions quand nous constatons un manque dans les solutions du marché. Par exemple, nous avons développé le portail pour les patients car nous avons considéré que les solutions disponibles sur le marché n'étaient pas facilement intégrables ou n'offraient pas les services qui nous intéressaient. S'agissant du développement du portail pour les patients, nous avons opté d'emblée pour la *security by design* et la *privacy by design*. Cela signifie que les équipes de développement, le RSSI et la DPO sont intégrés dans le cycle de développement. S'agissant de l'entrepôt de données de santé, nous intégrons également ces enjeux plus en amont. Cela n'est pas simple. Nous intégrons donc les enjeux de sécurité dans notre cahier des charges et dans notre expression de besoins.

La cybersécurité couvre un sujet beaucoup plus large que celui de nos propres développements. Les dernières attaques montrent que les hackers n'ont pas attaqué un logiciel du marché : ils se sont introduits par des portes dérobées, par des vulnérabilités de logiciels d'infrastructure. Ils n'ont pas attaqué un dossier patient informatisé. Ils sont entrés par une porte, qui était ouverte pour un tas de raisons, et se sont introduits plus avant dans le système. Il faut y réfléchir.

Nous avons mis en place beaucoup d'outils de sécurité. Nous possédons une bonne sécurité périmétrique : cela signifie qu'entrer et sortir de l'AP-HP est compliqué. Nous avons recours pour cela à des outils classiques du marché : nous avons, par exemple, investi, sur le

volet antivirus, dans Vade Secure, qui est une entreprise lilloise. Nous possédons quelques très bons acteurs français en la matière mais nous avons du mal à les valoriser. Vade Secure fait partie des leaders mondiaux sur le sujet. Nous avons opéré un vrai choix afin de soutenir une entreprise française. S'agissant de la cybersécurité, l'AP-HP recourt à des outils classiques, conduits des audits – cela est très insuffisant de mon point de vue, mais ce sujet est devenu très prégnant depuis deux ans.

M. Philippe Latombe, rapporteur. Je souhaitais vous interroger sur le code des marchés publics. Lors de son audition, Mme Stéphanie Combes nous a expliqué qu'aucun appel d'offres n'avait été lancé pour le Health Data Hub, mais que si un appel d'offres avait été lancé, Azure de Microsoft aurait été la seule solution en mesure de répondre. Vous expliquez, de votre côté, que vous cherchez à élargir le spectre des solutions à utiliser. Comment composez-vous avec le code des marchés publics pour atteindre cet objectif sans pour autant vous mettre en difficulté juridique ? Procédez-vous systématiquement à un allotissement ? Passez-vous des petits marchés ?

Dr Laurent Treluyer. Oui, nous faisons de l'allotissement. Auparavant, nous passions de gros marchés de 20 ou 25 millions d'euros. L'allotissement nous a permis de diversifier nos fournisseurs et de disposer d'une expertise beaucoup plus pointue, en recourant à des entreprises spécialisées plutôt qu'à un opérateur très généraliste qui sous-traite.

Le code de la commande publique est une contrainte. Nous sommes passés par une centrale d'achat pour acheter Vade Secure. Il existe trois centrales d'achat public dans le domaine de la santé : l'Union des groupements d'achats publics (UGAP), le Réseau des acheteurs hospitaliers (RESAH) et la Centrale d'achat de l'informatique hospitalière (CAIH). Ces centrales d'achat passent des appels d'offres. Une grande partie de nos achats se font par leur intermédiaire afin de bénéficier de leur expertise juridique et technique.

Le code de la commande publique interdit de favoriser une entreprise française ou européenne. La situation est différente dans les autres pays : Joseph Biden, dès son investiture, a renforcé le *Buy America Act* et a obligé les organismes fédéraux à acheter américain. Aux États-Unis, l'achat public constitue une vraie politique, pour des raisons économiques et pour des raisons de souveraineté. Nous ne possédons pas, en France, ces outils-là. Quand nous lançons un appel d'offres, nous pouvons essayer d'y inclure des éléments qui permettront d'orienter les réponses, mais en réalité, toutes les entreprises peuvent être compétitrices.

En matière de cybersécurité, nous sommes opérateurs de services essentiels et nous avons par conséquent déclaré des systèmes d'information essentiels. Nous pouvons donc exiger que certains éléments soient référencés auprès de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Cela nous permet, en partie, d'orienter nos commandes. Mais c'est encore compliqué et cela cause également des problèmes en matière de coûts.

M. Philippe Latombe, rapporteur. L'AP-HP a atteint une masse critique assez importante. Vous devez également, je l'imagine, rencontrer vos homologues des CHU ou des centres hospitaliers européens de taille similaire à la vôtre. Ont-ils, eux aussi, les mêmes difficultés en matière de commande publique ? Ou bien la France est-elle la seule à limiter les marges de manœuvre en raison du code de la commande publique ?

Dr Laurent Treluyer. Nous sommes clairement confrontés aux mêmes sujets que nos collègues français. En matière de comparaison avec nos collègues européens, je ne connais pas les situations et les législations applicables en matière de commande publique en Europe. Nous collaborons avec différents collègues européens dans une organisation rassemblant neuf

grands CHU européens, mais nous n'avons pas abordé ensemble la question de la commande publique.

M. Philippe Latombe, rapporteur. Existe-t-il des solutions techniques françaises ou européennes qui seraient utilisées par des centres hospitaliers européens et dont vous ne disposez pas ? Autrement dit, un écosystème se crée-t-il autour de vos activités en France et en Europe ?

Dr Laurent Treluyer. Nous ne savons pas orienter notre commande publique afin de favoriser le développement d'un écosystème français ou européen. Cela constitue, à ma connaissance, un sujet important. Il est plus difficile de discuter avec un donneur d'ordre américain qu'avec un donneur d'ordre français. Je suis très souvent contacté par des commerciaux représentant des donneurs d'ordre américains. Les commerciaux sont sous pression et il est, à la vérité, impossible de discuter avec le vrai donneur d'ordre. Nous avons certainement une plus grande capacité à agir si le donneur d'ordre est en France ou en Europe.

Il s'agit également de savoir comment nous pouvons faire émerger des idées de nos CHU et les valoriser. L'antivirus Vade Secure est le fruit du travail de chercheurs sur l'intelligence artificielle en France. Ils ont cherché à mettre en place une rupture technologique autour de leur outil, s'agissant notamment du *phishing*, et ont créé une vraie compétence. Ils ont ouvert un bureau en France, à Lille, et un bureau à Boston, et génèrent maintenant un chiffre d'affaires confortable. Il est important de savoir comment nous pouvons les aider. Il est plus facile, pour nous, d'avoir un donneur d'ordre en France qu'aux États-Unis. L'Europe est très ouverte en la matière, à la différence des autres pays comme la Chine, les États-Unis ou la Russie.

M. Philippe Latombe, rapporteur. Je souhaite revenir sur les logiciels que vous utilisez. Avez-vous opéré ces choix technologiques car votre fonctionnement est décentralisé ? L'AP-HP rassemble 39 établissements. Vos choix technologiques dépendaient-ils de ce fonctionnement décentralisé, notamment du point de vue de la standardisation des données ?

Mme Elisa Salamanca. Ces éléments ne sont pas complètement corrélés. Le Dr Laurent Treluyer l'a expliqué : nos systèmes d'information sont partagés – c'est le cas, par exemple, du dossier patient informatisé. Nous avons donc commencé par nous appuyer sur ces logiciels et sur les données qu'ils contenaient pour constituer l'entrepôt de données de santé de l'AP-HP. Les solutions techniques mises en place pour exploiter les données découlent de cette stratégie de mise en réseau. Nous étions soucieux de créer une offre de service centrale pour tous nos utilisateurs. Mais je ne pense pas que cette question ait guidé nos choix au début.

La question s'est en revanche posée en matière de gouvernance : il s'agissait de savoir comment gérer ces 39 hôpitaux, qui possèdent tous une culture de gestion de la donnée différente et entre lesquels existe toujours, forcément, une compétition interuniversitaire. Les questionnements sur la centralisation et la décentralisation ont donc été plus importants en matière de gouvernance et de règles d'accès aux données. Ces questionnements persistent aujourd'hui. Face aux initiatives historiques de certains de nos hôpitaux – à titre d'exemple, un entrepôt de données de santé existe dans l'un des hôpitaux de l'AP-HP depuis plus de dix ans –, il s'agit pour nous de savoir comment offrir le même niveau de service à tous les chercheurs.

M. Philippe Latombe, rapporteur. S'agissant de la gouvernance, vous avez mis en place un comité scientifique et éthique réunissant des médecins, des chercheurs, des paramédicaux, des représentants de patients. Disposer d'une telle instance était-il important

en matière de management et de culture au sein de l'AP-HP, notamment pour favoriser l'acceptation de l'entrepôt de données de santé et son utilisation ?

Mme Elisa Salamanca. Cela était essentiel. Ce comité a été parmi l'un des premiers points abordés, lorsque nous avons lancé le projet en 2015. Nous avons rassemblé la communauté médicale et les représentants de patients afin qu'ils se donnent des règles communes pour partager ces données. Sans ces règles communes, notre entrepôt de données de santé n'aurait pas pu connaître un tel essor.

Ces questions sont encore aujourd'hui présentes : nous avons dernièrement refondu les règles d'accès de notre entrepôt de données de santé ; cela a été discuté avec les collégiales médicales de l'AP-HP et la présidente du CSE. Ces sujets sont essentiels. Ils permettent de faire émerger un débat sur ce qu'est un entrepôt de données de santé, quelles règles nous lui fixons et quels objectifs sont poursuivis avec l'utilisation de ces données. Il est normal de discuter régulièrement de ces sujets car cela constitue une des conditions d'acceptation du projet. Des chercheurs vont déposer des demandes d'accès aux données de l'entrepôt parce que des règles d'accès ont été partagées et que les utilisateurs sont en phase avec la manière dont les données sont utilisées. La gouvernance était essentielle pour que le projet puisse se développer.

Dr Laurent Treluyer. Dès le départ, nous avons défini non seulement des règles d'accès à la donnée, mais aussi d'information et d'utilisation des données. Nous avons également récemment rediscuté des règles de publication. Ces éléments sont extrêmement importants pour nos médecins et pour nos professeurs des universités et praticiens hospitaliers (PUPH). Nous avons voulu intégrer dans cette gouvernance des lieux de discussion. Nous n'aurions pas pu mener à bien ce projet sans cette gouvernance et sans le travail du professeur Marie-France Mamzer, qui a été essentiel. Nous ne pouvons pas nous en passer. Nous avons d'ailleurs été le premier entrepôt de données de santé à être autorisé par la CNIL, et ce point a été souligné par la CNIL dans son autorisation.

M. Philippe Latombe, rapporteur. Quelles discussions menez-vous aujourd'hui sur la valorisation des données et qu'en attendez-vous ? La construction d'un entrepôt de données de santé et sa maintenance ont évidemment un coût. Comment est-il possible de valoriser les données collectées ?

Dr Laurent Treluyer. Cette question fait partie des débats qui ne sont pas complètement clos avec le Health Data Hub. Pour nous, valoriser ne signifie pas vendre la donnée, car nous n'en sommes pas propriétaires. Il n'existe pas de propriété de la donnée. Nous sommes dépositaires des données de santé de l'AP-HP.

Il convient, pour pouvoir la valoriser, de disposer d'une certaine masse critique de données. Il faut également que la donnée atteigne un certain niveau de qualité. Les équipes de Mme Elisa Salamanca travaillent à ce que la donnée soit formatée, standardisée, facilement utilisable. Ce travail d'extraction et de mise à disposition de la donnée est un travail extrêmement important, qui doit être valorisé.

Nous travaillons dans un CHU. Nous collectons des données, certes, mais qu'en faire ? Si la donnée alimente la recherche en matière d'algorithmes d'intelligence artificielle, il est encore besoin de tester ces algorithmes. La compétence de notre CHU consiste donc à produire de la donnée, à la valoriser, puis à tester cette valeur. Notre rôle n'est pas de créer des algorithmes d'intelligence artificielle – nous pouvons le faire, mais nombre de start-up peuvent également le faire. En revanche, qui va tester l'algorithme d'intelligence artificielle pour savoir s'il est correct ? Enfin, nous nous interrogeons pour savoir comment intégrer ces outils

dans le parcours clinique d'un patient. Il faut intégrer les algorithmes dans les outils existants et dans le parcours de soin des patients. Ce sont ces éléments que nous souhaitons valoriser.

Il n'est donc pas question de dire : « Nous possédons dix millions de scanners et nous vendrons trois euros chaque scanner pour atteindre un revenu de trente millions d'euros ». Cela n'est pas le sujet. Au contraire, il s'agit de valoriser les activités d'un CHU avec toutes ses compétences : à la fois les compétences informatiques, de *data scientists*, de valorisation de la donnée et les compétences en recherche clinique. L'AP-HP réunit des personnes qui produisent de la donnée et des chercheurs cliniques. Cette confrontation permanente, qui s'incarne dans la notion de campus, crée de la valeur.

Nous voulons conserver notre avance en la matière et pour cela, nous avons besoin d'investissements. La question, pour nous, est de savoir comment intégrer de plus en plus de données. La France accuse un énorme retard dans la collecte de données, par exemple des données de pathologies numériques, car nous ne numérisons pas nos *labs*, à la différence des autres pays européens. Notre capacité d'intégration et de valorisation de la donnée est en revanche excellente. Mais nous avons des besoins supplémentaires pour intégrer de nouvelles données, les valoriser et travailler ensemble pour avancer encore davantage.

Mme Hélène Coulonjou. J'abonde dans le sens des propos du Dr Laurent Treluyer. Pourquoi est-ce qu'un CHU investit-il autant de temps et d'argent dans un entrepôt de données de santé, et dans ses données de vie réelle en général ? Cela conditionne l'attractivité du CHU pour nos médecins et chercheurs, et donc l'amélioration de la prise en charge des patients. Dans un second temps, il s'agit d'améliorer la soutenabilité de tous ces dispositifs que nous créons autour des systèmes d'information.

Il faut faire fi de cette croyance selon laquelle nous sommes assis sur un tas d'or et que nous pouvons vendre les données brutes. Les laboratoires pharmaceutiques sont largement revenus de ce type d'expérience. La donnée brute n'a aucune valeur : elle n'a de valeur que qualifiée par l'expertise clinique et outillée par des algorithmes ou des instruments issus de la mathématique appliquée.

L'AP-HP a largement travaillé avec les acteurs industriels sur l'intelligence artificielle et la valorisation des données de santé, dans l'élaboration du contrat stratégique de filière des industries et technologies de santé. Cela a donné lieu à un travail assez intéressant. Les équipes qui gèrent la propriété intellectuelle en matière de recherche et les collaborations y ont travaillé. Nous sommes partis d'assez loin avec les industriels sur le sujet de savoir comment, pourquoi et de quelle manière valoriser la donnée de santé. Nous étions les seuls représentants publics hospitaliers. Parmi les acteurs publics, l'Institut national de la santé et de la recherche médicale (Inserm) était également présent dans ce groupe sur l'intelligence artificielle. Nous sommes arrivés à des positions relativement conciliables. Nous avons conclu que nous pouvions tirer un parti mutuel de la valeur de cette donnée de santé. Ces débats sont complexes, et il est important qu'ils aient pu exister et qu'ils existent encore.

La collaboration avec les acteurs privés se fait de manière très concrète dans des projets de recherche et développement en santé qui sont largement fondés sur des données massives et des données de vie réelle. Le dernier et le plus probant de ces projets est le projet AI DReAM, dont le coût total s'élève à 55 millions d'euros et qui est financé par Bpifrance. Il réunit pour les hôpitaux l'AP-HP, Gustave Roussy, l'Institut Curie et l'hôpital Saint-Joseph à Paris. Il est piloté par GE Healthcare avec d'autres acteurs industriels. Ce projet travaille sur l'image avec cinq cas d'usage. Nous avons, dans ce projet, réussi à créer une infrastructure pour la donnée image à trois niveaux :

– les entrepôts de données au sein de chacun des établissements de santé, avec la possibilité pour l'établissement de continuer à travailler sur la donnée acquise et outillée, pour d'autres usages que ceux prévus par le projet ;

– une plateforme constituée par l'industriel GE Healthcare, qui produit de l'algorithme et qui procède, par exemple, à de l'automatisation de *contouring* d'images ;

– le dernier niveau consiste à verser au catalogue du Health Data Hub des jeux de données standardisés issus du projet – il s'agit d'un engagement pris envers Bpifrance. Ce type de valorisation est donc possible.

D'autres formes de valorisation sont également possibles : l'AP-HP a noué depuis plus de deux ans un partenariat avec la start-up française d'intelligence artificielle Owkin. Le partenariat est fondé sur l'apport mutuel. Owkin entraîne ses modèles sur des données de santé de l'AP-HP et à l'issue de cet entraînement, la valeur créée par ces modèles et par les produits logiciels qui en découlent est partagée selon un ratio 50-50. Ce type de modèle de valorisation existe dans le cadre de collaborations.

Nous travaillons enfin à l'idée de créer une offre de services qui permettrait de proposer des prestations, en particulier à l'industrie pharmaceutique, sur la base des trois piliers suivants : de la donnée de haute qualité, de l'expertise clinique et un environnement clinique adapté pour le calcul sur les données.

M. Philippe Latombe, rapporteur. Quels sont vos projets-phares, et comment pouvons-nous, parlementaires, vous aider dans la conduite de ces projets ? Vous manque-t-il des outils législatifs et réglementaires pour poursuivre les travaux que vous avez entamés ?

Mme Hélène Coulonjou. Le Dr Laurent Treluyer a évoqué la difficulté d'effectuer le chaînage avec les données du SNDS, notamment celles issues de nos recherches cliniques prospectives. Au cours de la crise, nous avons créé une cohorte massive de patients porteurs du virus SARS-CoV-2 et cela n'a toujours pas abouti. Il nous semble que la CNIL se situe aujourd'hui dans une pratique de surinterprétation du règlement général sur la protection des données (RGPD). Suivant le ratio bénéfices-risques, cela condamne beaucoup de recherches en santé. J'ai conscience que ce que je dis est délicat, mais je ne sais pas l'expliquer autrement. S'agissant des données de soins de patients pris en charge par l'AP-HP, les patients sont informés par tous moyens que leurs données de soins peuvent être réutilisées à des fins de recherche. Ils sont également informés du fait qu'ils ont le droit de s'y opposer. Pourtant, lorsque la CNIL statue sur un projet de recherche, elle demande des choses impossibles, comme de réinformer individuellement chacun des patients dont les données de soins sont prêtes à être réutilisées dans une recherche. Cela constitue un obstacle important.

M. Philippe Latombe, rapporteur. Quelle est la profondeur des données dont vous disposez au sein de l'entrepôt de données de santé ? Il est compréhensible qu'il soit besoin de réinformer un patient si celui-ci a donné son accord, il y a dix ans. La profondeur des données peut donc générer le besoin de réinformer les patients.

Dr Laurent Treluyer. Nous disposons de données de plus de dix ans, et nous pouvons accéder à des données jusqu'à quinze ans en arrière. Il est difficile de réinformer des patients d'il y a quinze ans : un certain nombre d'entre eux sont décédés ou bien nous ne possédons plus leurs coordonnées à jour.

L'autorisation de la création de l'entrepôt de données de santé accordée par la CNIL prévoit la possibilité de montrer que l'AP-HP a fait tous les efforts possibles pour se conformer

au RGPD. L'entrepôt de données de santé a été agréé par la CNIL dans ces conditions. Nous entretenons de vrais débats avec la CNIL : cela est normal et notre collaboration est plutôt bonne sur l'ensemble des sujets.

Le SNDS ne dépend pas seulement de la CNIL. Je dispose de beaucoup de données nominatives personnelles, et j'ai l'impression qu'accéder à des données pseudonymisées ou anonymisées est impossible. Il faut, pour cela, mettre en place des dispositifs de sécurité extrêmement importants. Il existe une hypersensibilité sur le sujet qui nous rend les choses compliquées. Les CHU n'ont pas été extrêmement favorisés dans la facilitation des accès au SNDS et dans le décret qui en découle.

S'agissant de la souveraineté, la commande publique est un vrai choix politique. Nous devons atteindre un équilibre dans l'ouverture par rapport aux États-Unis, à la Chine et à la Russie qui sont nos principaux compétiteurs en matière numérique. Ces pays opèrent des choix très différents des nôtres. Restons-nous toujours très ouverts ou pouvons-nous aider nos entreprises à émerger ? L'un des facteurs pour encourager cette émergence est la commande publique. Le président Joseph Biden a clairement exprimé que le budget annuel de 600 milliards de dollars de la commande publique serait utilisé pour soutenir les entreprises américaines. Nous ne devons pas être exclusifs, car nous ne pouvons pas acheter européen en tout domaine, mais nous devons pouvoir favoriser, dans nos choix, le soutien aux entreprises européennes. Sur le long terme, il est plus facile et plus intéressant que nos donneurs d'ordre soient en France pour créer une vraie collaboration de plusieurs années avec eux. Ces débats se présentent sans cesse à nous.

Notre budget est trop faible, et nous avons du mal à trouver des fonds. L'entrepôt de données de santé a été construit car le directeur général a décidé d'allouer des fonds à ce projet. Nous avons ensuite bénéficié de dons et d'aides. Il est compliqué d'investir. Or l'investissement conditionne notre capacité à faire. Cela fait partie des débats que nous avons eus avec le Health Data Hub : il est de l'intérêt du Health Data Hub, de notre intérêt et de l'intérêt de la France de constituer un véritable réseau de hubs régionaux. Nous avons vraiment besoin de votre aide dans ces débats.

Enfin, la France souffre de son absence au niveau européen. L'Europe va investir beaucoup d'argent dans les sujets d'innovation et de santé. Comment accéder à ces budgets ? Nous sommes très mauvais dans l'accès aux subventions européennes. Nous étudions actuellement comment construire une stratégie d'influence en la matière, et notamment constituer des consortiums avec nos collègues. Nous devons absolument y arriver. Nous laisserons passer des montants importants, si nous ne sommes pas organisés dès maintenant pour répondre aux projets européens.

Mme Hélène Coulonjou. Lorsque la directive européenne sur la commande publique a été transcrite en France, Bercy avait oublié que les établissements de santé étaient des acheteurs et ne les avait par conséquent pas consultés. L'organigramme de la direction du budget ne comprend aucun bureau pour les hôpitaux. Or, le montant des achats des établissements de santé en France est considérable.

Au-delà du retour sur investissement que pourrait dégager une stratégie d'influence auprès des institutions européennes, je note également l'intérêt d'une synergie avec nos collègues européens. L'intérêt mutuel sur la donnée, et la donnée de santé en particulier, est absolument majeur.

Audition, ouverte à la presse, de M. Dominique Pon, responsable ministériel du numérique en santé (*4 mars 2021*)

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Nous poursuivons nos auditions sur la souveraineté numérique et les données de santé en recevant M. Dominique Pon, responsable ministériel du numérique en santé et directeur général de la clinique Pasteur de Toulouse.

La stratégie Ma santé 2022 a été présentée par le Président de la République et par la ministre des solidarités et de la santé en 2018. Elle a été reprise au sein de la loi du 24 juillet 2019 relative à l'organisation et à la transformation de notre système de santé. Cette loi a encouragé le déploiement de la télémédecine et du télésoin, a prévu la création d'une plateforme de données de santé – le Health Data Hub – ainsi que la possibilité pour chaque usager d'ouvrir un espace numérique de santé (ENS) d'ici le 1er janvier 2022. Nous sommes heureux d'échanger avec vous, M. le directeur général, sur l'état d'avancement de ces différents projets et la manière dont ils intègrent l'impératif de souveraineté numérique.

M. Philippe Latombe, rapporteur. Je souhaite vous interroger sur trois points en particulier.

Je souhaiterais tout d'abord que vous nous présentiez un état d'avancement de la stratégie Ma santé 2022. Notre mission d'information portant sur le thème de la souveraineté numérique, j'aimerais savoir comment vous appréhendez cet enjeu et de quelle façon vous l'intégrez au sein de vos choix techniques. Cela nous permettra de revenir sur le lancement du Health Data Hub et en particulier sur le choix de recourir au *cloud* de Microsoft. J'aimerais également savoir si vous avez été confronté, en pratique, au même type d'arbitrage au sein des projets dont vous avez la charge et quelle a été, le cas échéant, votre doctrine pour trancher entre les différentes offres disponibles.

Le deuxième point concerne la gestion et la protection des données de santé. L'actualité récente est marquée par des cyberattaques contre les systèmes d'information des établissements de santé. Face à la sophistication de la menace cyber, comment est-il possible, selon vous, de garantir un niveau de protection maximale à nos infrastructures numériques, en particulier dans le domaine de la santé ?

Enfin, le dernier point concerne la formation aux technologies du numérique en santé. Votre action témoigne de l'importance croissante du numérique et des technologies de pointe pour la prise en charge des patients. Selon vous, quelle est la place du numérique dans les formations de santé ? Quels progrès envisagez-vous grâce à la numérisation de notre système de santé ?

M. Dominique Pon, responsable ministériel du numérique en santé. Nous publions chaque année un document de bilan portant sur l'ensemble de la feuille de route du numérique en santé. Nous nous astreignons chaque année à la transparence quant aux engagements que nous avons pris en avril 2019. Nous tenons, à la semaine près, la totalité des engagements compris dans cette feuille de route qui regroupe cinq orientations et trente actions extrêmement concrètes. Nous dépensons, Mme Laura Létourneau, la totalité des équipes et moi-même, une énergie folle pour tenir, à la semaine près, les engagements pris. Cette feuille de route définit

un cadre d'action et d'orientation allant jusqu'à la mi-2022. Nous irons au bout et nous ferons ce que nous avons promis.

Je rappellerai le principe général de la feuille de route. Son point de départ est le rapport présentant un état des lieux du numérique en santé en France préparé par Mme Annelore Coury et moi-même. Je m'occupe du pilotage national de la stratégie du numérique en santé et je suis également directeur d'établissement. Depuis vingt ans, je suis confronté à la réalité du numérique en santé en France. Je constate qu'en la matière, nous naviguons entre le fantasme et la frustration. Nous fantasmons les apports positifs du numérique en santé, mais nous sommes incapables d'être humbles, pragmatiques, de décider d'actions claires, d'avancer collectivement et dans la durée. Beaucoup d'autres pays ont adopté une approche beaucoup plus humble que la nôtre, ont moins fantasmé le numérique et avancent depuis quinze ans, brique après brique, pour construire un système numérique de santé cohérent.

Ces quinze dernières années, je constate qu'il n'y a eu aucune doctrine, aucun portage politique, aucun volontarisme : chacun a développé ce qu'il souhaitait – les régions, les hôpitaux, les professionnels de santé, les industriels, les start-up. Sans socle commun, sans référentiel commun, sans logiciels communiquant entre eux, aucune règle n'existe aujourd'hui pour garantir la sécurité suffisante des données de santé. Les professionnels de santé sont extrêmement frustrés car ils sont confrontés à des ruptures dans les parcours de soin, puisque les logiciels ne communiquent pas entre eux. Le citoyen, lui, n'a toujours pas accès à ses informations de base et à ses données de santé en ligne pour devenir acteur de sa santé.

Dans ce contexte, plusieurs choix étaient possibles. La feuille de route du numérique incarne le parti-pris selon lequel il n'existe pas d'homme, ni de femme, ni de logiciel providentiel pour résoudre la totalité des sujets du numérique en santé en France. La meilleure façon d'avancer est d'adopter une posture humble et extrêmement pragmatique. Il nous faut fixer un cadre de valeurs et une vision communs, dans lesquels nous obligerons l'ensemble des acteurs à s'inscrire. Nous sommes un peuple frondeur et dans l'autodénigrement permanent. Nous devons donc imposer une vision. L'État est le seul acteur capable de réguler, d'organiser tout cela et de proposer des services numériques socles.

Nous proposons donc le cadre de valeurs suivant :

– tout d'abord, nous devons être redevables d'une stratégie de résultats qui s'inscrit dans un cadre de valeurs souverain. Je crois à la souveraineté nationale et européenne en matière de numérique en santé ;

– ensuite, le numérique en santé ne doit pas concerner seulement les professionnels : il doit également concerner les citoyens. Le numérique en santé doit être directement orienté vers les citoyens. Nous devons proposer des plateformes numériques pour le citoyen français ;

– enfin, le cadre éthique du numérique en santé n'est pas seulement lié à la souveraineté et qu'au Règlement général sur la protection des données (RGPD). L'éthique doit être la marque européenne et française du développement du numérique en général, et du numérique en santé en particulier.

Notre cadre de valeur se résume donc par ces trois points clés : souveraineté, citoyenneté, éthique.

Nous portons également une vision. Elle consiste à demander à l'ensemble des acteurs qui développent des outils numériques de converger vers des référentiels-socles construits par l'État et imposés à l'ensemble des acteurs. Ces référentiels socles comprennent, par exemple,

un téléservice permettant de créer une identité numérique de base pour chaque citoyen et de s'échanger des données de santé. Cela est désormais fait. Cela comprend également le référencement des professionnels de santé dans des annuaires proposés par l'État ainsi que des référentiels des terminologies de santé. L'État arbitre, il fixe le cadre – s'inscrivant pour cela dans un référentiel international et européen – et l'impose à tous les acteurs. L'État construit également des briques techniques en matière de cybersécurité imposées à l'ensemble de l'écosystème.

Le cœur du dispositif est l'espace numérique de santé. Il s'agit d'une plateforme souveraine portée par l'État, permettant à chaque citoyen français de gérer ses données de santé, de donner des consentements d'accès à ses données de santé, de posséder une adresse de messagerie sécurisée pour ses données de santé, de posséder un agenda santé et d'avoir accès à un catalogue numérique d'applications développées par l'écosystème et référencées par l'État dans l'espace numérique de santé du citoyen. Cette plateforme constitue réellement le point clé de toute notre stratégie. Pour être souverain, l'État doit créer les fondations du numérique en santé en France. Il doit construire la plateforme – le contenant –, ouverte et destinée au citoyen, et référencer les services numériques qui ont accès à cette plateforme. Je suis profondément convaincu que nous sommes en train de construire ce qui va nous permettre d'être souverains en matière de numérique en santé.

M. Philippe Latombe, rapporteur. S'agissant de la souveraineté, le Health Data Hub a fait le choix de recourir à un *cloud* américain, à savoir la solution Azure de Microsoft. Nous avons auditionné le Ouest Data Hub et l'AP-HP : ils sont tout à fait favorables au Health Data Hub, mais ils portent une vision différente et mettent en avant un souci de souveraineté. Pourquoi donc avoir fait le choix de recourir à un *cloud* américain pour le Health Data Hub ? Ce choix ne représente-t-il pas un boulet dans la construction de votre stratégie ?

M. Dominique Pon. Cela est compliqué. Je suis redevable des actions dont j'ai la responsabilité, et la totalité de ces actions s'inscrit dans une stratégie régalienne et souveraine – c'est le cas, par exemple, de l'espace numérique de santé. La seule action dont je n'ai jamais eue la responsabilité est le Health Data Hub. Or, vous me questionnez à ce sujet.

S'agissant de la situation du Health Data Hub, je comprends que la commande politique donnée exigeait de construire une plateforme d'hébergement des données de santé dans un *cloud,* à très court terme et avec un niveau de sécurité très élevé. Cela signifie que, dans tous les cas, la commande politique court-termiste conduisait au choix d'un *cloud* qui n'était pas souverain. À l'état de l'art, compte tenu des délais et des exigences de sécurité donnés, il n'était pas possible de faire le choix d'un *cloud* souverain. Si j'avais moi-même reçu la commande politique, j'aurais lutté du mieux possible pour faire comprendre que la commande politique n'était pas la bonne. La bonne commande politique suppose de se donner davantage de temps et de construire un *cloud* souverain avec quelques industriels européens. J'aurais alors demandé si la commande politique pouvait évoluer. En matière de numérique en santé en France, depuis mes prises de fonction, j'ai milité et tenu bon en faveur du modèle souverain. Alors que quand je parlais de la notion de souveraineté, il y a cinq ans, j'étais considéré comme un « ringard ».

M. Philippe Latombe, rapporteur. Je veux bien vous croire. Le sens de ma question est le suivant : la caisse nationale d'assurance maladie (CNAM) a fait savoir par communiqué de presse qu'elle refusait de transmettre ses données aux Health Data Hub. Cela a forcément des impacts sur l'avancement de votre stratégie. Je vous interroge donc sur les conséquences de ces choix sur l'ensemble de la stratégie de Ma santé 2022.

M. Dominique Pon. Cette affaire du Health Data Hub est le symptôme d'une maladie française. Nous fantasmons le fait de devenir l'un des leaders du numérique en santé, mais la réalité est que nous ne disposons pas des bases souveraines pour le faire. Je milite pour une solution souveraine, pragmatique, humble, progressive et collective. Nous devons construire notre modèle humblement et pas à pas, sans chercher à copier des modèles libertaires à l'américaine ou autocratiques à la chinoise. Nous devons fixer un cadre éthique et souverain pour le numérique. Évidemment, nous n'aurons pas instantanément un *cloud* du niveau d'Amazon ou de Microsoft, mais nous attirerons des talents car nous créerons du sens autour du numérique, dans la tradition humaniste et éthique européenne.

Je milite donc pour que nous fixions d'abord ce cadre de valeurs. Il faut pour cela faire preuve d'humilité : nous ne serons pas capables de tout faire tout de suite. Nous avons dix années de retard sur les Américains en matière de numérique. Le modèle du futur n'est pas forcément *« big »*, il consiste avant tout à réussir à donner du sens au numérique. L'humanisme numérique est l'avenir. Il créera de la valeur. Nous attirerons les talents si nous tenons bon dans cette vision. Cela nécessite d'être humbles.

M. Philippe Latombe, rapporteur. Je partage en grande partie votre position. Un ensemble d'auditions précédentes a relayé l'idée selon laquelle la commande publique ne permet pas l'émergence d'un écosystème ni de favoriser des solutions françaises et européennes. Ressentez-vous également cela au quotidien dans votre métier de « terrain » ? Avez-vous pris cela en compte dans l'élaboration de la stratégie ?

M. Dominique Pon. Je dirige une clinique privée, mais je suis extrêmement attaché au bien commun et à l'État. Je suis désormais en immersion dans l'administration et je comprends ses contraintes et ses lourdeurs.

Si l'exigence d'être souverains est réellement portée, si émerge une conscience citoyenne que la souveraineté est essentielle pour sauvegarder notre système de santé, notre modèle de société, notre tradition de pensée, alors je crois qu'un mouvement se déclenchera qui amènera également de nouvelles clauses dans les appels d'offre pour les hôpitaux publics. Je pense que nous finirons donc, malgré tout, par y arriver. À mes yeux, il a manqué, depuis dix ans, une vision politique durable qui définit ce cadre de valeurs. Cette vision politique a toujours été floue ; cela explique le cadre actuel des marchés publics. Nous nous intéressons aux problématiques de souveraineté seulement récemment et après-coup.

Construire notre souveraineté numérique est possible. Les services numériques de la stratégie Ma santé 2022 existent aujourd'hui dans un cadre souverain. L'espace numérique de santé que nous construisons avec l'Assurance maladie sera souverain. Cette action est peut-être humble ; mais elle constitue une brique fondamentale pour construire notre souveraineté numérique du futur. Nous devons donc fixer un cap sur le long terme et cesser de changer de direction.

M. Philippe Latombe, rapporteur. Comment faudrait-il donc faire pour élaborer cette stratégie et la maintenir dans le temps ? Cela nécessite-t-il selon vous des changements organisationnels ?

M. Dominique Pon. Quand Mme Annelore Coury et moi-même avions rédigé notre rapport, nous nous étions demandés : qui dirige le numérique en santé en France ? La seule solution de court-terme, que nous avions trouvée alors, était la création d'une délégation ministérielle. La délégation pilote les différentes agences : l'agence du numérique en santé, les équipes de l'Assurance maladie, l'agence technique de l'information sur l'hospitalisation (ATIH), les agences régionales de santé (ARS). Cela permettait de poser clairement une

responsabilité et de savoir qui arbitre et définit une vision. Le problème a donc été partiellement résolu par la création de cette délégation ministérielle du numérique en santé.

Je pense néanmoins que ces enjeux mériteraient la création d'une direction centrale. Le numérique n'est pas seulement un outil : il constitue une stratégie en soi. Nous avons pour l'instant créé une délégation ministérielle. Cela a déjà beaucoup amélioré la capacité de coordination. Nous avons construit une vision commune, et les échelons territoriaux, régionaux et nationaux sont alignés et travaillent ensemble.

Comment faire pour que cela perdure dans le temps ? Je n'en sais trop rien. Ma conviction profonde est qu'il faut impliquer le citoyen français. Dès lors que le citoyen français disposera d'un espace numérique de santé et qu'il commencera à comprendre les enjeux liés au numérique en santé – notamment depuis la crise COVID –, il donnera un cap politique. Le cap politique apportera la pérennité – voilà ce que j'espère.

M. Philippe Latombe, rapporteur. Faut-il impliquer le citoyen français en l'obligeant à entrer dans le système tel que vous l'avez défini, ou faut-il l'amener à entrer dans le système de façon volontaire ? Une partie de la population est réfractaire à ces questions du numérique. Certains enjeux ne sont aujourd'hui pas bien perçus. Faut-il imposer un système au citoyen ou bien montrer les avantages du système pour susciter son intérêt ? Par exemple, le dossier médical partagé n'a pas trouvé le succès que l'on espérait au départ.

M. Dominique Pon. Je m'exprime avec mes mots – que cela ne soit pas mal reçu. En France, nous infantilisons trop les citoyens. Nous ne responsabilisons pas les citoyens, nous les infantilisons. Il faudrait bien plutôt dire aux gens : voilà où l'on en est et cela n'est pas parfait ; et les interroger : quel modèle de société voulons-nous ? Nous restons passifs, à moitié fascinés et à moitié effrayés par ce que font les géants du web – Google, Apple, Facebook, Amazon et Microsoft (GAFAM). Ne voulons-nous pas plus humblement construire un système souverain ? L'État n'est-il pas le meilleur tiers de confiance qu'un citoyen puisse avoir, même si celui-ci n'apprécie pas son gouvernement ? Ne peut-on pas proposer aux citoyens de construire ensemble – l'État, les professionnels de santé et les citoyens – un système qui leur permette de se réapproprier les enjeux du numérique en santé ? Ce discours doit être transparent. Il ne doit pas annoncer le Grand Soir. À ma connaissance, ce discours n'a jamais été tenu.

Nous avons commandé une enquête Opinion Way pour présenter aux Français le principe de l'espace numérique de santé et ses fonctionnalités. À la question « Préférez-vous que ce projet soit porté par un acteur privé ou par l'État ? », 80% des personnes interrogées préfèrent l'État. Cette question n'avait jamais été posée publiquement auparavant. À la question « Que pensez-vous de ses fonctionnalités ? », les résultats montrent deux préoccupations majeures : la sécurité des données et l'inclusion numérique. L'État doit montrer qu'il essaie, avec les acteurs de terrain, de progresser vers l'inclusion numérique. Ce discours, non infantilisant, constitue la première étape. Le volet coercitif ne peut pas précéder ce débat citoyen que nous n'avons jamais organisé sur le numérique en général, et sur le numérique en santé en particulier.

M. Philippe Latombe, rapporteur. Faut-il donc généraliser ce débat citoyen ? Doit-on organiser un débat sur le numérique en général, dont le numérique en santé est une des composantes ?

M. Dominique Pon. Cela constitue, à mes yeux, le point clé. Nous jouons notre modèle de société, notre tradition de pensée et notre cadre de valeurs. Les modèles libéraux et libertaires à l'américaine ne correspondent pas à notre culture. La France a connu le siècle des

Lumières et l'essor des Droits de l'Homme. Sans aucun jugement de valeur, cela n'est pas notre tradition de pensée. Il est ultra pragmatique de tenir ce débat pour essentiel.

En tant que directeur d'établissement de santé, j'ai pleuré pendant la crise du COVID que nous ne soyons pas capables de fabriquer des masques, des circuits clos de respirateurs, des *stents* de cardiologie ou des valves chirurgicales. Je sais que, de la même manière, mes enfants pleureront demain que nous n'ayons pas fait le travail nécessaire pour être souverains en matière de numérique.

M. Philippe Latombe, rapporteur. Comment amorceriez-vous le débat avec les citoyens ?

M. Dominique Pon. Cela doit faire partie de l'éducation populaire. Dès lors que l'on commence à expliquer l'idéologie sous-jacente aux outils numériques américains, les gens comprennent très bien les enjeux. Ce sujet est accessible. Il faudrait aborder ces enjeux par les canaux d'éducation populaire normaux, en parler sur des chaînes de télévision grand public. Cela devrait faire partie de notre responsabilité collective car nous jouons notre modèle de société pour les dix prochaines années. Le numérique se démocratise et il entraîne avec lui de nouveaux enjeux. Il faut faire confiance aux gens : ils sont capables de comprendre, d'appréhender les enjeux et de se positionner. Nous avons tous la responsabilité – les politiques, les journalistes, les citoyens, les associations – d'introduire ce débat populaire sur cet outil majeur pour notre liberté.

M. Philippe Latombe, rapporteur. Comment est aujourd'hui vécu le numérique dans la population des soignants ? Constitue-t-il une contrainte ou un outil d'avenir ?

M. Dominique Pon. Il est extrêmement difficile de faire des généralités : je ne me prononcerai donc pas. Je vous répondrai par un exemple. Les personnes qui s'expriment sur le numérique dans le secteur de la santé expriment tout d'abord des frustrations.

Il y a dix-huit ans, j'ai été embauché à la clinique Pasteur de Toulouse comme informaticien. Un schéma directeur du numérique avait été élaboré par la société de conseil Ernst & Young. J'y ai opposé une autre solution : j'ai proposé de construire notre propre dossier patient informatisé, d'en faire une start-up, d'industrialiser cette solution, puis de la déployer dans d'autres établissements en France. Nous l'avons fait. L'ensemble des professionnels de santé ne croyait pas possible de créer notre propre dossier patient informatisé. Ce processus a pris du temps, il a donc fallu rester humble et gérer les frustrations des professionnels de santé. Plusieurs années après, les médecins considèrent cet outil comme indispensable et se prononcent tous en faveur de la numérisation. La première phase est donc la résistance, puis s'en suivent la frustration et enfin la réussite et la capacité à développer une activité.

Ensuite, nous avons proposé de développer un outil pour les patients. À nouveau, les professionnels de santé ont opposé de la résistance. Le taux d'adhésion des patients à cet outil a été d'environ 90%, alors même que la moyenne d'âge des patients se situait autour de 65 ans. L'outil leur a simplifié la vie et nous avons mis en place des métiers numériques de soignants qui humanisent l'outil. La résistance s'est donc dissipée, alors que le lancement du projet avait suscité un tollé auprès des professionnels de santé.

Dès lors qu'ils constatent la sincérité dans les engagements et les valeurs, et dès lors qu'ils sentent que l'outil dispose d'une vraie capacité à être utilisé dans le réel, les professionnels de santé accompagnent le changement. Il faut cependant faire preuve de sincérité, d'engagement et montrer des valeurs humanistes et de terrain. Cela est vrai dans le

numérique et cela est vrai dans tous les secteurs. Il faut recréer la confiance collective dans le fait que nous allons nous en sortir.

M. Philippe Latombe, rapporteur. Faisons-nous suffisamment de place au numérique dans les études des praticiens de santé ? Dressons-nous suffisamment les perspectives d'évolutions de leurs métiers à l'horizon de quinze ou vingt ans grâce à l'essor du numérique en santé ? N'avons-nous pas intérêt à faire évoluer les programmes pédagogiques des professionnels de santé pour y intégrer les enjeux du numérique ?

M. Dominique Pon. Cela constitue à mes yeux un point clé. Le numérique manque cruellement aux formations. Mais nous ne pourrons consacrer une plus grande part au numérique dans les études des professionnels de santé que si nous disposons d'une vision claire de ce que nous voulons pour le numérique en santé en France. Nous ne pourrons proposer une offre claire de formation au numérique, incluant des outils concrets pour les professionnels de santé, que si nous optons pour une feuille de route et un socle de valeurs communs et clairs, par exemple, construire un numérique placé directement au service du citoyen. Pour intégrer le numérique dans les programmes de formation, il faut au préalable avoir défini notre cadre de valeurs et notre vision pour le numérique. Sinon, cela revient à fragmenter à nouveau une vision collective, car aucun cadre n'a été fixé pour les programmes. Il ne suffit pas de dire que le numérique est important, qu'il va changer les métiers de la santé grâce à l'intelligence artificielle. Il faut d'abord cadrer la vision et les objectifs que nous poursuivons grâce au numérique.

M. Philippe Latombe, rapporteur. Pour élaborer la stratégie Ma santé 2022, vous êtes-vous inspiré des modèles européens ou étrangers dont vous avez jugé l'architecture convaincante ? À titre d'exemple, la vaccination contre le COVID a montré qu'Israël disposait d'un système de numérique en santé très intégré, qui permettait aux laboratoires de dresser des retours d'expérience très rapides sur les effets de la vaccination. La stratégie Ma santé 2022 inclut-elle aussi des référentiels européens ou internationaux ?

M. Dominique Pon. Nous avons inclus des référentiels, mais pas des modèles. Je commencerai par une anecdote. Il y a trois ans, un patient de 75 ans venant de Bilbao en Espagne et passant ses vacances à Toulouse est hospitalisé en urgence dans mon établissement. Vivant à 300 kilomètres au sud de Toulouse, il m'a montré sur son *smartphone* ses antécédents médicaux, son traitement en cours, son pilulier virtuel. Ce genre de solutions n'existe pas en France. En Espagne, l'équivalent des espaces numériques de santé est déjà opérationnel. J'ai donc creusé le sujet et j'ai étudié les stratégies en vigueur en Belgique et au Danemark. J'étais par ailleurs allé me former en tant que directeur d'établissement aux États-Unis.

Tous ces modèles concrets reposent sur un système citoyen et sur une reprise en main du cadrage par l'État. Je me suis donc posé la question de savoir comment adapter cela à notre culture et nos valeurs. Imposer un système unique (par exemple, imposer à tous les médecins généralistes un même logiciel) n'est pas possible en France, compte tenu de notre tradition de pensée et de notre culture. J'en suis donc venu à la conclusion que tous les logiciels existants doivent se baser sur les mêmes briques régaliennes. En France, il est impossible de réformer au point d'uniformiser de manière autocratique. Cela n'est pas du tout en phase avec notre culture. Nous proposons donc la logique d'État-plateforme : l'État fournit la plateforme et les industriels fournissent les briques à y intégrer.

M. Philippe Latombe, rapporteur. Quels éléments sont aujourd'hui manquants d'un point de vue législatif ou réglementaire pour avancer dans la construction de la stratégie Ma santé 2022 ? Doit-on modifier, faire évoluer, supprimer des freins législatifs ou réglementaires ?

M. Dominique Pon. Je constate absolument partout des manques réglementaires. Je n'identifie pas un point central qu'il conviendrait de modifier pour tout régler. Il existe de nombreuses incohérences dans les textes réglementaires : puisqu'aucune vision n'était portée, tout s'est construit par strates, par décrets et par arrêtés qui ne sont pas cohérents les uns avec les autres.

La feuille de route inclut un important volet juridique pour rendre tous ces éléments cohérents. Nous avons aujourd'hui besoin de davantage des fonctionnaires sur ces sujets. Il nous manque de la main d'œuvre compétente pour accélérer les réponses à tous ces manques et rendre tous les textes cohérents.

M. Philippe Latombe, rapporteur. Ce que vous construisez actuellement en matière de données de santé peut-il être mutualisé avec d'autres domaines ? Votre méthode pourrait-elle être déployée dans d'autres domaines et si oui, lesquels ?

M. Dominique Pon. Cela est sûr et certain.

M. Philippe Latombe, rapporteur. Puisque nous ne disposons pas, hélas, d'un ministère du numérique transversal, comment pouvons-nous donner envie à d'autres ministères de s'inspirer de votre méthode et de votre stratégie ?

M. Dominique Pon. Ma conviction profonde est que tous les principes de conduite du changement mis en œuvre dans ce modèle peuvent être dupliqués. À mes yeux, les ressorts essentiels en sont les suivants :

– tout d'abord, un cadre de valeurs porté de manière sincère ;

– ensuite, une forte présence sur le terrain pour convaincre et définir une vision commune ;

– enfin, une fondation constituée de quelques briques techniques fixées par l'État, dans une logique ouverte à l'écosystème afin que l'innovation portée par le système privé vienne compléter les services numériques de l'État.

Ce modèle peut se répliquer dans l'éducation, la justice, la recherche – dans quasiment tous les domaines.

L'autre point clé est la numérisation des démarches administratives, avec un seul identifiant. La notion d'espace numérique de santé pourrait être un espace numérique citoyen. Général, il pourrait regrouper une brique pour les données administratives, une brique « santé », une brique « éducation », et ainsi de suite. À mes yeux, l'objectif final est de proposer ce type de service aux citoyens. L'État apporterait à ce sujet une garantie à l'écosystème, grâce à un catalogue numérique d'applications développées par l'écosystème et référencées par l'État dans l'espace numérique. Toutes les démarches administratives, tous les identifiants, tous les sujets clés de la vie quotidienne pourraient être rassemblés dans cet espace numérique, dont l'État proposerait le socle de base, sans en développer tous les services numériques. Cela serait le modèle du futur en France. Cette proposition est ultra basique, mais nous en avons besoin.

M. Philippe Latombe, rapporteur. Quelles sont, pour vous, les perspectives du numérique en santé en France, en Europe et dans le monde ? Quelle sera la place du numérique en santé dans dix ans et à quoi servira-t-il ?

M. Dominique Pon. Ma réponse n'est pas basée sur une analyse objectivée et prospectiviste. Mon ressenti est que l'usage du numérique en santé par le citoyen constituera le futur. Cela dépassera les avancées de l'intelligence artificielle. Les investissements, partout dans le monde, pour proposer des applications citoyennes de santé créeront un impact réel et feront bouger les lignes. J'en veux pour exemple le boom des *digital therapeutics* – cela constitue d'ailleurs une filière industrielle forte en France. À mes yeux, l'avenir du numérique est de se développer du côté des usages du citoyen : cela recouvre les applications de détection précoce des maladies, de prévention, d'auto-surveillance, de lien avec son médecin, de gestion de son parcours de soin impliquant le patient lui-même et tous les usages de la médecine 4P (personnalisée, préventive, prédictive, participative).

M. Philippe Latombe, rapporteur. L'actualité récente rapporte de nombreux cas de cyberattaques sur des établissements de santé. La protection informatique des hôpitaux et des cliniques est-elle au niveau en France ?

M. Dominique Pon. Je peux vous assurer que n'importe quel hacker déterminé peut casser n'importe quel système d'information d'un hôpital en France – y compris mon établissement, et pourtant, nous faisons tout ce que nous pouvons en la matière. Nous sommes fragiles. Ce sujet n'a jamais été une priorité pour les directeurs généraux. Cette préoccupation est très récente.

Je milite pour conduire un exercice « Plan blanc » dans tous les établissements de santé : cela permet de tester en réel nos capacités à continuer à soigner, sans avoir accès à aucun service numérique. À mes yeux, un tel exercice constitue le B.A-BA. Mais cela n'a jamais fait partie des priorités nationales, car la maturité et les connaissances des enjeux du numérique font défaut. Nous sommes fragiles et il faut donc y mettre les moyens : il faut acculturer les personnels, il faut créer des compétences. Il est extrêmement difficile de recruter des personnels compétents en matière cyber dans les hôpitaux publics. Bien souvent, les grilles de salaires ne permettent pas de recruter des personnes compétentes.

La cybersécurité et la sécurité des systèmes d'information se construisent sur des années. Cela constitue un travail de long terme. Cela nécessite de travailler tout un tas de sujets dans une démarche d'amélioration continue. Nous sommes en retard en la matière.

M. Philippe Latombe, rapporteur. Il n'y a donc pas de plan de continuité d'activité en cas de cyberattaque ?

M. Dominique Pon. Cela ne fait pas partie des exercices demandés dans les plans blancs. Nous allons l'inclure dans les exercices obligatoires. De mon propre chef, j'avais décidé de conduire dans ma clinique des exercices de simulation « sans informatique dans les services ».

Un autre point extrêmement important en matière de cybersécurité concerne la centralisation des données. Ce sujet donne lieu à des débats que je juge un peu immatures. En France, l'on a souvent peur que la centralisation des données cause une atteinte aux libertés individuelles. Il faudrait expliquer que nous sommes en mesure de donner un maximum de gages de sécurité sur les données recentralisées. Nous ne pouvons pas garantir qu'il n'y aura jamais aucune faille. Mais nous pouvons garantir que nous avons tout fait pour rendre le système le plus sécurisé possible. Puisque le débat sur la centralisation suscite des peurs, nous préférons fermer les yeux et répartir nos données dans divers lieux, qui créent des « passoires » de sécurité partout. Ce sujet n'a jamais été abordé franchement. Les gens pourraient comprendre qu'il y a un intérêt à centraliser certaines données dans un lieu sécurisé. Ce débat

n'a jamais été tenu, et cela donne donc lieu à des débats immatures portant sur les peurs et les libertés individuelles.

M. Philippe Latombe, rapporteur. Y a-t-il un sujet que nous n'avons pas abordé et que vous souhaiteriez évoquer ?

M. Dominique Pon. J'aborderai un dernier point extrêmement important. Sur ces sujets, nous sommes un peuple qui a perdu confiance en lui. Nous mettons en œuvre un mécanisme de défense par rapport à cette perte de confiance dans notre modèle : l'autodénigrement. Nous croyons que nous n'y arriverons pas, nous pointons constamment ce qui ne marche pas. Ce comportement est névrotique. Une de nos responsabilités collectives – les parlementaires en particulier, mais aussi les médias – est de changer de principe. Nous devons revenir à un principe d'humilité, en ayant confiance dans nos valeurs et en mettant en avant les avancées positives, les réussites de terrain. Cela peut nous redonner une dynamique de construction positive. Ce comportement, que je constate dans les discours et dans les politiques publiques, pose un problème très profond à mes yeux. Nous en souffrons énormément dans le numérique.

M. Philippe Latombe, rapporteur. Il faut donc raconter des belles histoires pour donner l'envie d'avancer.

M. Dominique Pon. Oui, de belles histoires réelles. Il faut mettre en avant les héros du quotidien, les gens de terrain qui réalisent des actions qui s'inscrivent dans le cadre de valeurs que nous souhaitons pour notre pays. Ils sont nombreux. Il faut les mettre en lumière.

M. Philippe Latombe, rapporteur. Si vous avez de très bons exemples, nous les rencontrerions avec plaisir.

Audition, ouverte à la presse, de M. Olivier Micheli, président de DATA4 *(4 mars 2021)*

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Nous poursuivons nos auditions sur le thème de la souveraineté numérique et des données, en recevant M. Olivier Micheli, président directeur général de DATA4 et de France Data Center, association professionnelle rassemblant les principaux acteurs de cette filière. Nous nous réjouissons de pouvoir échanger avec vous, afin de mieux connaître cette filière et évoquer les moyens de soutenir son développement en France et en Europe.

Je souhaiterais d'abord vous interroger sur trois points.

En premier lieu, que recouvre pour vous la notion de souveraineté numérique ? Ce sujet fait l'objet d'une attention croissante de la part des pouvoirs publics depuis la crise sanitaire, et nous avons eu l'occasion d'entendre, au cours de nos auditions, plusieurs définitions de cette notion très large, que certains rapprochent parfois d'une forme d'autonomie stratégique, ou d'autonomie décisionnelle. J'aimerais donc savoir comment vous appréhendez cette notion, en tant qu'acteur clé du stockage et de la sécurisation des données.

En second lieu, j'aimerais que vous nous présentiez la filière française des *data centers*, dont vous constituez un acteur important. Comment appréhendez-vous la situation actuelle, marquée par la crise sanitaire et la volonté de tous les États de promouvoir leur souveraineté numérique ? Quelle est la situation de DATA4, et plus généralement des acteurs de ce secteur d'activité ? Quelles sont vos éventuelles difficultés, et vos propositions pour renforcer le rythme d'installation des *data centers* en France ? Je m'interroge également sur les échanges que vous pouvez entretenir avec vos homologues européens. La structuration d'une filière des *data centers* européenne est-elle envisageable à terme ?

Enfin, au regard de l'actualité récente, marquée par des cyberattaques sur les systèmes d'information des établissements de santé, et face à la sophistication de la menace, quels risques pèsent sur les *data centers* et comment assurent-ils la protection des données qu'ils stockent ?

M. Olivier Micheli, président de DATA4. Ma définition de la souveraineté numérique s'articule autour de deux volets, l'un défensif, l'autre offensif.

D'un point de vue défensif, la souveraineté numérique signifie qu'il est important de conserver la maîtrise opérationnelle du numérique. En cas de crise (de fermeture des frontières, de tension internationale, etc.), il faut s'assurer que les entreprises, les administrations et les citoyens aient toujours accès à leur environnement numérique, et notamment à leur environnement numérique essentiel. En d'autres termes, les entreprises pourront-elles continuer à fonctionner en temps de crise ? Auront-elles accès à leurs applications et à leurs données sans trop de difficultés ?

D'un point de vue offensif, la question est de savoir comment créer des champions numériques européens. La plupart des acronymes connus pour désigner les champions du numérique renvoient à des entreprises étrangères : les GAFAM aux États-Unis ; les BATX en Asie et notamment en Chine. Quand un tel acronyme renverra-t-il à des acteurs majeurs, connus et puissants, du numérique en Europe ?

Il est essentiel de travailler sur ces deux volets.

Disposer de *data centers* localisés en France constitue à cet égard une composante incontournable de la souveraineté numérique.

Le numérique est souvent considéré comme virtuel, de sorte que la question de la localisation des données ne semble pas se poser. En simplifiant à l'extrême, le numérique peut être décomposé en trois couches : les infrastructures numériques, incluant les réseaux et les *data centers* ; les équipements informatiques, incluant les serveurs et les systèmes d'exploitation (qui sont hébergés dans les *data centers*) ; enfin les applications, que nous utilisons quotidiennement. Les applications étant installées sur des serveurs, qui sont hébergés dans des *data centers*, il est indispensable que ces derniers soient bien maîtrisés. Ils constituent le socle du numérique, et si nous soulignons la nécessité de disposer de *data centers* en France, c'est qu'il est important de pérenniser ce socle sur le sol français, afin, premièrement, ne pas dépendre d'un acteur tiers qui pourrait décider de l'accès ou non aux *data centers* en cas de crise.

Deuxièmement, il est essentiel de maîtriser la qualité et la continuité du service assuré par les *data centers*. Un *data center* doit fonctionner jour et nuit, 24 heures sur 24. Or, sans électricité, les *data centers* ne fonctionnent pas. Nous maîtrisons en France le réseau électrique français. Nous connaissons ses forces et ses faiblesses. Nous connaissons son état. En revanche, nous ne maîtrisons pas l'état des réseaux électriques dans les autres pays. En Afrique du Sud, par exemple, des coupures d'électricité ont lieu tous les jours. Par conséquent, les *data centers* n'y peuvent fonctionner que sur des groupes électrogènes. Tous les pays d'Europe ne sont certes pas dans cette situation. En tout cas, les *data centers* doivent reposer sur des réseaux électriques fiables et pérennes.

Troisièmement, un *data center* nécessite des capitaux considérables. Il crée des emplois directs et de très nombreux emplois indirects, avec un impact économique fort. Pourquoi laisser ces capitaux partir à l'étranger, alors que la France, du fait de ses atouts (sur lesquels nous reviendrons plus loin), a la capacité d'en attirer énormément pour construire des *data centers* sur son sol ?

Quatrièmement, conserver les *data centers* en France permettra d'y disposer d'un bon niveau de connaissances et de compétences. Un *data center* suppose des techniciens qualifiés et des ingénieurs. Il permet de regrouper au sein d'un même bâtiment un grand nombre de compétences : des ingénieurs et des techniciens spécialisés en génie mécanique et en électricité, des informaticiens, des ingénieurs en télécommunications, des ingénieurs méthodes, etc. Si les *data centers* partent à l'étranger, la France perdra autant de personnes qualifiées sur ces sujets clés.

Pour toutes ces raisons, nous pensons donc qu'il est essentiel de conserver des *data centers* en France.

De plus, nos voisins européens s'organisent. Ils ont compris l'importance des *data centers*. Ils ont compris que les infrastructures numériques comprenaient les réseaux de télécommunications, qui sont clés, mais aussi les *data centers*, et ils cherchent désormais à attirer des capitaux pour en construire davantage sur leurs territoires.

La filière des *data centers* en France dispose d'abord d'une très belle association professionnelle, France Data Center, qui comprend plus de 100 membres. Elle existe depuis douze ans et est aujourd'hui très bien organisée, puisqu'elle regroupe l'ensemble des acteurs majeurs du *data center* en France. Elle a pour objectif à la fois de développer des

connaissances et des savoirs, de partager des bonnes pratiques et de travailler à des sujets clés comme l'optimisation de la consommation électrique, l'impact environnemental, etc.

200 *data centers* commerciaux, mutualisés pour un grand nombre de clients, sont localisés en France, d'une manière qui reflète parfaitement l'organisation très centralisée de notre pays, puisque 75 % de l'activité des *data centers* est réalisée à Paris et en région parisienne. C'est là que les développements les plus importants ont lieu, même si des développements plus modestes existent aussi en région.

Au total, la France compte environ 5 000 *data centers*, en comptant les *data centers* commerciaux et tous les *data centers* privés : ceux des collectivités locales, des administrations, des entreprises, etc., pour lesquels des salles blanches de quelques mètres carrés seulement sont parfois nécessaires. Cette filière est très active. Elle investit beaucoup, à hauteur d'environ un milliard d'euros chaque année sur le territoire français.

Par ailleurs, la France a la chance de disposer de champions mondiaux dans le secteur des *data centers*, et ce, sur l'ensemble de leur chaîne de valeur : en amont, avec les concepteurs et constructeurs avec Schneider, Saft (très belle société de batteries), Bouygues, Imogis, etc. ; ensuite au niveau de la maintenance en condition opérationnelle des *data centers* avec Engie ; enfin, en aval, avec les opérateurs utilisateurs. Or, pour être fort à l'international, il est important d'être fort au niveau national. Pour conserver ces leaders, il est donc essentiel de disposer d'un marché domestique puissant du *data center* en France, puisqu'il permettra à ces écosystèmes et à ces champions de se développer, de produire de la R&D, et ainsi de s'exporter encore davantage à l'international.

S'agissant de la crise sanitaire, les deux vagues de confinement n'ont pas impacté le secteur de la même manière.

La première vague, de mars-avril 2020, a été difficile à gérer, pour différentes raisons. L'ensemble de l'activité économique de construction a d'abord été arrêtée brutalement. Or, si arrêter des chantiers aussi complexes que ceux des *data centers* est difficile, les reprendre l'est encore plus : redémarrer un chantier implique des pertes de productivité considérables. Le maintien en conditions opérationnelles des *data center*s a été difficile également, car un *data center* ne cesse jamais de fonctionner. DATA4 a donc été obligée de faire venir sur site des employés spécialisés, malgré la crise sanitaire. Or, en mars 2020, la situation était mal connue, les kits de protection étaient peu nombreux et l'anxiété relative à la pandémie était très grande. Nous avions alors demandé au gouvernement son soutien plein et entier à l'égard de notre secteur d'activité. Il s'était en effet engagé auprès des opérateurs de télécommunications, mais non auprès des opérateurs de *data centers*, et il nous était essentiel de pouvoir continuer à circuler pour accéder à nos *data centers*. Une grande confusion en avait résulté, même si nous avons finalement réussi à gérer la situation.

Une fois la première crise sanitaire passée, la deuxième vague n'a en revanche pas eu le même impact sur la filière et sur DATA4, et la situation est désormais bien maîtrisée.

Surtout, le trafic internet a augmenté de 30 % durant la crise sanitaire. Du jour au lendemain, toutes les organisations (entreprises privées ou publiques, etc.) ont adopté le travail à distance, et la filière a garanti une continuité de service sans rupture sur l'ensemble du territoire, en parfaite transparence pour l'ensemble des citoyens, des organisations, de l'administration, des collectivités locales, etc. Tout le monde a pu continuer à travailler à distance grâce aux *data centers*, et nous en sommes naturellement très fiers.

Vous me demandiez également comment renforcer la filière des *data centers* en France.

M. Philippe Latombe, rapporteur. Je vous le demandais, parce qu'il résulte de l'arrêt *Schrems* II, notamment, une volonté de stocker les données sur le territoire national ou européen. S'agit-il pour vous d'une opportunité à investir rapidement, et de quelle manière ?

M. Olivier Micheli. Oui, complètement.

La France dispose d'atouts magnifiques. Son territoire est parfaitement adapté au développement des *data centers*, qui constituent des bâtiments techniques hébergeant des serveurs sur lesquels reposent des applications telle que Zoom, que nous utilisons actuellement.

Une grande quantité d'énergie est donc nécessaire pour alimenter ces serveurs (qui fonctionnent à l'électricité), mais aussi leurs groupes de refroidissement, car ils dégagent une chaleur considérable. Des réseaux de télécommunication sont enfin requis, puisqu'un *data center* est une « maison du numérique », où les données sont stockées, traitées et renvoyées vers les différents utilisateurs. La France dispose d'une grande quantité d'énergie décarbonée, à un prix compétitif. Le prix de l'électron est beaucoup plus compétitif en France qu'en Allemagne ou en Italie, en Angleterre, etc. C'est une chance.

Les risques naturels doivent être limités également. La France connaît certes des risques d'inondation, mais son climat est tempéré d'une manière générale, et les risques sismiques y sont faibles. Ils sont plus importants dans d'autres pays voisins.

La France dispose également de bonnes formations, et de deux hubs internet majeurs, à Paris principalement, mais aussi à Marseille, car les routes de l'internet suivent approximativement les anciennes routes commerciales. L'axe Paris-Marseille (ou Marseille-Paris) regroupe ainsi 80 % du trafic internet entre l'Europe et trois régions majeures : l'Afrique, le Moyen-Orient et l'Asie du Sud-Est. La plupart des câbles de ces régions passent en effet par le canal de Suez, remontent par la Méditerranée, avant de s'arrêter en Grèce et en Sicile, puis à Marseille. C'est une grande chance pour la France. Or, là où passent les câbles internet, des *data centers* sont nécessaires.

Pour autant, des freins existent également au développement des *data centers* en France. Il a notamment besoin de stabilité, de prévisibilité et de cohérence dans les politiques publiques. En 2019, la réduction de près de 50 % de la taxe sur l'énergie consommée dans les *data centers* leur a permis de gagner en compétitivité en France, et d'y devenir plus compétitifs que dans certains pays voisins. Deux ans plus tard, toutefois, ce prix préférentiel a été soumis à des conditions très impactantes pour le secteur : mettre en place un système de gestion de l'énergie ; faire partie d'un groupement de bonnes pratiques en consommation de l'énergie ; etc. La réglementation peut donc changer très rapidement en France. En l'occurrence, la loi de finances a évolué. La question est donc de savoir quelle sera l'étape suivante. Ce nouveau cadre sera-t-il pérenne ? Nos investissements se font sur un temps long. Un *data center* dure près de quarante ans. Il est donc essentiel que les politiques publiques soient stables et cohérentes.

Le décret Tertiaire pose également problème. Il n'est pas du tout adapté aux *data centers*, puisqu'il vise à réduire le nombre de kilowattheures consommés dans les *data centers*, ce qui est impossible. Il n'est pas possible de supprimer des serveurs du jour au lendemain pour atteindre un objectif en valeur absolue défini par décret. Certains de ses critères ne sont

donc pas pertinents. Or, il est important que la réglementation soit cohérente avec l'activité des *data centers*.

Nos propositions sont donc les suivantes : il faut adapter le cadre administratif ; gagner en compétitivité pour attirer des capitaux (comme tous nos pays voisins le font) ; passer des commandes publiques aux acteurs français ; enfin, accorder aux *data centers* le statut d'infrastructure critique. D'autres crises que celle du Covid-19 auront lieu. Comme celle des opérateurs de télécommunications, l'activité des *data centers* doit être encadrée par un statut permettant de maintenir ces actifs en condition opérationnelle de manière permanente.

Chaque grand pays européen dispose de sa propre organisation professionnelle : l'Angleterre avec techUK, l'Allemagne avec eco, l'Irlande, la Hollande, bientôt l'Espagne et probablement l'Italie. Un ensemble d'actions de concertation et d'échanges ont déjà été lancées, au niveau européen, entre ces différentes organisations professionnelles, mais aussi à l'initiative du CISPE *(Cloud Infrastructure Services Providers in Europe)*, qui regroupe les acteurs du *cloud* en Europe. Une coordination européenne mensuelle a été mise en place, et des engagements forts de la profession sont constitués volontairement auprès de la Commission européenne, s'agissant notamment de la consommation électrique d'ici à 2025 et 2030.

S'agissant des cyberattaques, il est important de distinguer le contenant et le contenu. Les *data centers* ne sont qu'un contenant pour les serveurs et les applications, qui en constituent le contenu. Nous ne sommes pas responsables des applications hébergées par les clients dans nos *data centers*. La responsabilité de la sécurité logique des systèmes d'information que nous hébergeons revient aux administrations, organisations, etc. qui les possèdent. Pour autant, les opérateurs de *data centers*, et notamment DATA4, ont mis en place un programme complet de sécurisation physique et logique de leurs *data centers*. En ce qui concerne la sécurité physique, DATA4 a prévu plus de sept barrières de sécurité avant l'accès aux salles informatiques, avec des gardes, des systèmes de vidéosurveillance, etc. Des tests d'intrusion réelle sont réalisés chaque année dans l'ensemble de nos campus, pour tester leur sécurité physique. Un programme de sécurité logique est prévu également, avec des systèmes informatiques embarqués, et un cloisonnement strict entre différents réseaux : les systèmes d'information industriels (portant sur la gestion technique du bâtiment, par exemple) sont ainsi situés sur un réseau cloisonné et non accessible de l'extérieur. Naturellement, nous réalisons chaque année des tests de cyberattaque et nous disposons d'une équipe de plus en plus nombreuse de responsables de la sécurité des systèmes d'information, lesquels, en permanence, testent nos systèmes et étudient leurs failles de sécurité.

M. Philippe Latombe, rapporteur. Vous avez dit que 75 % des *data centers* commerciaux étaient situés à Paris. Est-ce lié à l'organisation des voies de l'internet que vous avez mentionnée, ou uniquement à des questions de compétences ou d'accessibilité ? Le numérique est souvent conçu comme une industrie d'avenir susceptible d'échapper à l'attractivité des grandes villes et de réindustrialiser les territoires ruraux. Les *data centers* commerciaux pourraient-ils donc être situés ailleurs qu'à Paris et créer ainsi un dynamisme économique dans des territoires qui en manquent, comme la Creuse, la Vendée ou l'Aveyron, etc. ?

M. Olivier Micheli. La première raison pour laquelle les grandes villes comme Paris, Francfort, Londres, Amsterdam, etc. rassemblent de nombreux *data centers* est qu'elles constituent des hubs majeurs où tout converge, et notamment les réseaux de télécommunications. Il est tout à fait logique, en effet, que les *data centers* se développent là où sont situés les grands « nœuds » Internet : à Madrid, Milan, Paris, Francfort, etc. Il est possible sur une carte de voir physiquement tous les réseaux de télécommunications converger

dans ces villes. Toutes les données y arrivent, et sont donc ensuite stockées dans des *data centers*.

La deuxième raison est économique. Les sièges sociaux des grandes sociétés françaises sont situés à Paris. Chaque région ou grande métropole en France accueille une grande société, mais Paris en concentre un nombre considérable. De très nombreuses équipes informatiques y sont donc également situées, et elles souhaitent que leurs équipements informatiques soient à proximité, afin qu'elles puissent y intervenir. Même si nous pouvons réaliser de nombreux gestes de proximité pour nos clients, eux-mêmes interviennent également sur site. Or, une société dont le siège social est situé à la Défense ou à Vélizy interviendra beaucoup plus rapidement sur un *data center* parisien que sur un *data center* situé dans la Creuse, à Lyon ou à Marseille, etc.

Vous avez parfaitement raison par ailleurs d'évoquer la question des compétences. Notre secteur est confronté à une réelle pénurie de compétences. D'ici 2025, cette pénurie est estimée dans le monde à près de 500 000 salariés spécialisés dans les *data centers*. Or, c'est à Paris que le plus grand nombre de personnes formées, compétentes et qualifiées (ingénieurs, techniciens, etc.) se trouvent. Ce n'est pas nécessairement là qu'elles sont les plus qualifiées, mais c'est là qu'elles sont les plus nombreuses.

Néanmoins, je crois beaucoup au développement des *data centers* en région. Ils n'atteindront certes pas la taille des « méga *data centers* », de plusieurs milliers de mètres carrés, que l'on trouve dans les grands hubs. Toutefois, pourquoi faire remonter les données de Lyon à Paris avant de les faire redescendre à Lyon, ou de Bordeaux à Paris avant de les faire redescendre à Bordeaux, etc. ? Les grandes villes françaises auront ainsi de plus en plus besoin de disposer de leurs propres *data centers*, de taille plus modeste, mais quand même importante, pour répondre aux besoins de leurs entreprises régionales, mais aussi aux besoins des villes et des territoires intelligents. En effet, tout se numérise : les entreprises, mais aussi les villes et les services, qui sont de plus en plus accessibles par l'intermédiaire de plateformes numériques. Et plutôt que d'être renvoyées vers de grands hubs comme Paris, les données afférentes devront être traitées localement, ne serait-ce que pour des raisons techniques de latence. Pour certaines applications (par exemple celles destinées aux voitures autonomes), le temps de latence entre l'émetteur et le récepteur doit ainsi être le plus court possible. Une distance de 400 kilomètres peut avoir un impact à cet égard. Si tout est traité au niveau de la ville même, le temps de latence sera réduit et la qualité du service encore améliorée.

Je suis plus dubitatif, en revanche, concernant la possibilité d'implanter des *data centers* dans des régions plus reculées comme la Creuse ou la Corrèze, etc. Je ne saurais toutefois me prononcer sur l'avenir au-delà de 2030. D'ici là, je prévois le développement de méga *data centers* dans les grands hubs, mais aussi de *data centers* de taille plus raisonnable dans les grandes villes et métropoles françaises.

M. Philippe Latombe, rapporteur. Vous venez d'indiquer que l'avenir des *data centers* tenait aussi à la numérisation des villes et des collectivités pour développer des « villes intelligentes », « smart cities », « données de la ville », etc. Quel développement des besoins en *data centers* la filière envisage-t-elle par cet intermédiaire : un développement exponentiel ou plus continu ?

M. Olivier Micheli. En premier lieu, la filière France Data Center ne s'appelle pas Paris Data Center, parce que nous y disposons d'acteurs présents sur l'ensemble du territoire (à Metz, Toulouse, Marseille, Lyon, etc.). Nous pensons donc fortement que l'avenir du *data center* en France impliquera bien toutes les régions, de Lille à Marseille. Ce point est donc parfaitement partagé.

En deuxième lieu, il faut bien comprendre que la production de données est en pleine « explosion ». En 2020, la Terre a produit en une année autant de données qu'elle l'avait fait au total jusqu'en 2020. Nous produisons et nous échangeons donc de plus en plus de données. Les *data centers* résultent alors de nos usages numériques. Plus nous produisons, plus nous avons besoin de stockage, donc de *data centers*. C'est ce que nous observons. Le développement des *data centers* est très important dans le monde, en Europe et en France, mais France Data Center pense que la France peut faire davantage. Elle dispose d'atouts magnifiques, mais présente aussi des freins, que j'ai évoqués. De plus, les *data centers* sont trop souvent mal compris, et ainsi perçus comme des actifs se contentant de rejeter de la chaleur non consommée dans l'atmosphère. Ils sont bien plus que cela. Un travail pédagogique important est à effectuer à cet égard, non pas tant auprès des citoyens qu'auprès du gouvernement, de l'administration et des élus, pour expliquer à quoi servent les *data centers* et pourquoi il est important d'en posséder. À condition de réaliser ce travail et de lever ces freins, les *data centers* ont de l'avenir partout en France.

M. Philippe Latombe, rapporteur. Les *data centers* sont de grands consommateurs d'électricité, ce qui est beaucoup reproché au numérique depuis quelque temps, maintenant que chacun sait chiffrer l'impact du numérique en termes de production de gaz à effet de serre et de consommation électrique. Investissez-vous dans la réduction de la consommation électrique ? Comment pouvez-vous « verdir » votre activité pour éviter ces critiques, conduisant à limiter le volume de données stockées et le recours aux *data centers*, qui nuirait à la planète ? Disposez-vous de pistes à cet égard ?

M. Olivier Micheli. La filière travaille depuis plus de quinze ans sur la réduction de son impact environnemental et l'optimisation de sa consommation électrique. Une étude publiée dans la revue *Science* a montré que, de 2010 à 2018, le nombre des serveurs a été multiplié par six, pour une augmentation de seulement 6 % de la consommation d'électricité des *data centers*, précisément parce que l'ensemble du secteur travaille à optimiser cette consommation. Elle y travaille d'abord pour une raison économique : la consommation électrique d'un *data center* représente 30 à 40 % de sa charge financière. La réduire impactera donc directement votre rentabilité.

La filière est également consciente de sa responsabilité. Elle constitue la partie émergée, visible, du numérique. Le numérique est souvent conçu comme virtuel, tandis que les *data centers* sont réels. Le *cloud* n'est pas situé dans les nuages, mais bien dans nos *data centers*, de manière très tangible et concrète. Il est donc facile de cibler les *data centers*, qui sont des actifs physiques et tangibles.

En matière de performance énergétique, il faut travailler à la fois sur la quantité et sur la qualité.

En termes de qualité, nous pensons qu'il est indispensable de se tourner de plus en plus vers les énergies renouvelables. Depuis 2007, 100 % de la consommation électrique de DATA4 est d'origine renouvelable. Nous avons mené cette conversion en France, en Italie, en Espagne et au Luxembourg, et nous continuerons en ce sens dans les prochains pays où s'étendra l'entreprise. À travers l'engagement volontaire PACTE pris auprès de l'Union européenne, des objectifs chiffrés nous sont fixés pour accroître d'ici 2025 et 2030 notre recours à l'énergie renouvelable.

S'agissant de la quantité d'énergie, les *data centers* de nouvelle génération de DATA4 utilisent l'air externe pour refroidir les serveurs hébergés dans leurs bâtiments. Le climat tempéré de la France le permet. Un air de très bonne qualité est également requis pour cette technologie, car les serveurs supportent très mal la poussière. L'air très pur dont nous

disposons sur notre campus de Marcoussis nous permet d'utiliser l'air externe 85 % du temps pour refroidir les serveurs hébergés dans nos salles informatiques. Cela nous a permis de réduire de près de 20 % la consommation électrique de nos bâtiments, de même que leur *power usage effectiveness* (PUE). Cet indicateur de performance énergétique rapporte l'énergie qui arrive dans le bâtiment à celle qui est utilisée par le serveur. La finalité d'un *data center* est en effet d'apporter de l'électricité à un serveur, pour qu'il puisse fonctionner. Plus ce rapport tend vers 1, plus votre *data center* est vertueux. Grâce à l'utilisation de l'air externe dans le cadre de notre technologie de *free cooling*, notre PUE est passé de 1,8 à 1,2, ce qui constitue un très bon niveau dans notre industrie. C'est donc sur ce type de technologies que nous travaillons pour réduire la quantité d'énergie consommée dans nos bâtiments.

DATA4 prône aussi très fortement une approche globale, « holistique », de l'ensemble du cycle de vie des *data centers* : de leur conception à la fin de vie des équipements, en passant par leur construction et leur exploitation. Le *free cooling* par exemple doit être intégré dès la conception. En construction, nous envisageons de recourir à des matériaux comme le béton vert. C'est en exploitation que des gains d'efficacité énergétique sont particulièrement possibles. Nous travaillons à cet égard sur des solutions consistant à compartimenter et cloisonner des allées de serveurs, pour concentrer la chaleur produite sur certains points précis, et y propulser l'air froid. Cela fait gagner considérablement en efficacité énergétique par rapport à une diffusion homogène de cet air.

La filière travaille donc depuis très longtemps à la fois sur la qualité et la quantité de l'énergie consommée, et sur l'ensemble du cycle de vie des bâtiments.

M Philippe Latombe, rapporteur. S'agissant de la cybersécurité, nous avons interrogé ce matin un spécialiste des données de santé. Selon lui, il n'existe pas aujourd'hui de plan de continuité d'activité dans les hôpitaux en cas de cyberattaque. Vous avez développé une expertise dans le domaine de ces plans de continuité d'activité. En cas de panne de courant, vous disposez de générateurs susceptibles de prendre le relais. Je suppose que vous avez également mis en place des mesures en cas de coupure des réseaux de télécommunications, et des plans de continuité d'activité en cas de cyberattaque, afin notamment d'isoler les points concernés et d'éviter ainsi la diffusion de l'attaque. Pourriez-vous partager ces compétences avec des acteurs stratégiques comme les hôpitaux, qui sont encore loin d'avoir suffisamment pris en compte ces considérations, alors même qu'ils stockent également des données, en l'occurrence dans des entrepôts de données de santé (EDS) ?

M. Olivier Micheli. L'association travaille beaucoup sur l'échange de bonnes pratiques. Elle est à cet égard ouverte à tous : collectivités locales, administrations, entreprises, etc. J'encourage les acteurs publics concernés (par exemple les hôpitaux de Paris, s'il s'agit d'eux) à nous rejoindre pour participer à ce partage, afin que les bonnes pratiques soient diffusées autant que possible.

La continuité de service constitue une question de moyens. Généralement, les données essentielles sont stockées sur un site primaire, et il est très important de se doter d'un site secondaire en cas de perte du site primaire, idéalement en « actif-actif », ce qui permet de répliquer les données du site primaire vers un site secondaire en temps réel, de sorte que le site secondaire reprend totalement la charge du premier, de manière parfaitement transparente. « L'actif-actif » s'oppose à « l'actif-passif » où cette réplication n'est pas en temps réel. Naturellement, se doter d'un site secondaire coûte cher, et se doter d'un site secondaire en « actif-actif » coûte encore plus cher. Tout dépend donc des moyens alloués. Pour les infrastructures et activités critiques, nous encourageons en tout cas la création de sites de secours. À DATA4, plusieurs sites sont disponibles et de nombreuses entreprises y installent leur informatique primaire sur un site et leur informatique secondaire sur un autre.

Au-delà du partage de bonnes pratiques, que nous pouvons proposer, des moyens financiers sont donc nécessaires, mais aussi des équipes compétentes en interne qui aient le temps et la capacité de mettre en place ce type de systèmes et surtout de les maintenir en conditions opérationnelles, ce qui prend beaucoup de temps.

M. Philippe Latombe, rapporteur. Vous l'avez évoqué : le *cloud* est lui aussi hébergé dans les *data centers*. Avec *Schrems* II, la possibilité d'utiliser des *clouds* souverains ou des *clouds* américains s'est posée. Quelle vision ont vos clients de l'utilisation du *cloud* ? Ont-ils commencé à s'interroger sur la localisation des données et la manière de les protéger et de les rendre souveraines au sens de *Schrems* II ? Ou s'agit-il encore pour eux d'une question mineure, par rapport à la recherche de solutions techniques et la question des coûts ?

M. Olivier Micheli. Ce n'est pas du tout une question mineure. Tous les clients se posent la question de la localisation des données. Une tendance de fond parmi les entreprises consiste à segmenter les données essentielles et les données accessoires. Une base de données client et les données de R&D notamment n'ont pas la même valeur que les données d'un site institutionnel Internet, même si ce dernier représente l'image d'une société. Selon qu'il s'agit des unes ou des autres, la perte n'a pas le même impact. Toutes les entreprises sont donc engagées dans la segmentation de leurs données, en fonction de leur niveau de criticité, et adaptent les environnements numériques de ces données à cette criticité.

Les réglementations entrent également en compte à cet égard. En Europe comme en France, la réglementation est ainsi très claire concernant le pourcentage d'informations pouvant être stockées dans le *cloud* ou non.

Il revient ensuite à chacun de déterminer où il localisera ses données en fonction de la segmentation retenue. Le « *cloud* privé » appartient à l'entreprise : il est hébergé dans ses propres machines et systèmes, fondés sur ses procédures propres, etc. Le « *cloud* public » quant à lui est hébergé par des plateformes mutualisées, que nous connaissons tous : il existe une très belle solution française, des solutions américaines, etc. Enfin, le « *cloud* hybride » consiste précisément à choisir entre le *cloud* privé et le *cloud* public en fonction de la criticité des données concernées.

Quelle est la définition d'un « *cloud* souverain », c'est-à-dire d'un *cloud* de confiance, permettant aux entreprises d'importance vitale, aux administrations, au gouvernement, de stocker leurs données en fonction de leurs besoins ? Je n'ai pas d'avis sur la question de savoir si son acteur doit être américain ou européen, etc. L'important est surtout qu'un *cloud* souverain doit fonctionner en autonomie, c'est-à-dire ne doit pas dépendre d'un État tiers, afin qu'il puisse continuer à fonctionner en temps de crise. Il doit également pouvoir fonctionner avec des ressources situées en France, ce qui signifie que des ressources capables de gérer les opérations du *cloud* doivent s'y trouver. Enfin, il est très important que les données soient localisées en France. Il faudrait très rapidement définir la notion de *cloud* de confiance, ou de *cloud* souverain, afin que différentes propositions y répondant (donc ne dépendant pas d'États tiers) soient rendues disponibles en France, ce qui ne signifie pas que leurs acteurs doivent tous être français. Une communication devrait alors être réalisée auprès des acteurs concernés, pour leur permettre d'héberger leurs données sur différents types d'infrastructures et de plateformes, en fonction de leur criticité.

M. Philippe Latombe, rapporteur. Il est fréquent d'entendre que les entreprises françaises ne sont pas suffisamment digitalisées ou numérisées, par opposition, par exemple, à l'Allemagne, en raison de la taille des entreprises, mais aussi de leur culture. Partagez-vous ce constat ? Vos *data centers* sont-ils principalement sollicités par des grands clients ou par

une multitude de petits comptes très atomisés, et la taille de vos clients a-t-elle évolué durant les dernières années ?

M. Olivier Micheli. Nous sommes présents dans différents pays européens voisins, et, si je connais moins la situation de l'Allemagne, la France n'a pas à rougir de sa situation par rapport à l'Italie ou à l'Espagne. Entre l'Europe du Sud et l'Europe du Nord, les pratiques sont toutefois différentes. Le recours à l'externalisation, notamment, est beaucoup plus fréquent en Europe du Nord qu'en Europe du Sud. Dans le domaine du numérique comme dans d'autres, les entreprises des pays du Sud sont ainsi plus réticentes à faire confiance à des sociétés tierces pour héberger et gérer leur informatique. Elles préfèrent s'en occuper elles-mêmes. Cet écart tend toutefois à se résorber sous l'effet des crises successives (financière, sanitaire, etc.) et de la compétition mondiale. Les entreprises ont besoin de se concentrer sur leur cœur de métier, et ont de moins en moins les moyens d'allouer des fonds importants à des activités pour elles accessoires. Elles font donc de plus en plus appel à des sociétés tierces pour gérer ces activités, et pouvoir ainsi concentrer leur énergie et leur capital à innover et se différencier sur leur cœur de métier.

Notre base de clients est très diverse. Nous travaillons avec la plupart des entreprises du CAC40, mais aussi avec de très belles entreprises de taille intermédiaire (ETI) et quelques PME. Nous travaillons donc avec des entreprises de toutes tailles, et toutes externalisent de plus en plus. Nous travaillons aussi avec des entreprises de la Tech, qu'il s'agisse d'intégrateurs, d'entreprises des services numériques (ESN) ou d'acteurs du *cloud*, et elles aussi externalisent beaucoup. De plus en plus, les entreprises font donc confiance à des acteurs spécialisés dans des télécommunications ou les *data centers* comme DATA4 pour externaliser leurs systèmes d'information.

M. Philippe Latombe, rapporteur. Au-delà des questions de taxation, y a-t-il selon vous des freins législatifs ou réglementaires à lever absolument pour améliorer l'écosystème numérique en France ?

M. Olivier Micheli. Je le répète : disposer d'une stabilité réglementaire est très important, car les investissements dans les *data centers* se font sur des temps très longs.

Par ailleurs, construire un *data center* en France est complexe en raison d'un cadre administratif parfois un peu long et lourd. Au-dessus de 400 mégawatts informatiques, par exemple, les installations classées pour la protection de l'environnement (ICPE) passent du régime de la déclaration à celui de l'autorisation. Or, le processus des autorisations ICPE est complexe, et surtout très long : il peut prendre un an. Déjà, construire un *data center* peut prendre dix-huit à vingt-quatre mois, du fait de la quantité considérable de technologie qu'abrite un tel bâtiment. Y ajouter douze mois de procédure ICPE constitue un frein supplémentaire. Il faudrait donc raccourcir ce délai d'autorisation, assez unique en Europe, pour des installations classées, au fond, bien connues.

D'autres obligations sont ensuite à remplir, d'une manière assez linéaire : après l'obtention du permis de construire et de l'autorisation ICPE, des fouilles archéologiques doivent être réalisées. Il ne s'agit pas de les mettre en cause : elles sont parfaitement légitimes, mais ne serait-il pas possible de les commencer avant, en engageant ainsi parallèlement les différentes procédures, pour gagner du temps ? Si des vestiges romains, etc. importants sont découverts, la poursuite des autres obligations administratives que doivent remplir les opérateurs de *data centers*, devenue inutile, aura ainsi pu être évitée. C'est donc surtout l'enchaînement linéaire des obligations administratives à remplir qui fait qu'elles prennent du temps. L'obtention du permis de construire prend trois mois, et quand on y ajoute le temps d'obtention d'une autorisation ICPE, etc., les délais deviennent extrêmement longs. Ce cadre

administratif n'est donc pas réellement adapté à notre type de développement, et nous gagnerions beaucoup à ce qu'il soit simplifié.

Enfin, comme je l'ai déjà dit, je souhaiterais que les *data centers* soient reconnus comme des infrastructures critiques et soient soutenus en cas de crise, afin que nous n'ayons pas à craindre qu'une limitation de circulation nous empêche d'accéder à nos bâtiments, et qu'un accès prioritaire au fuel, etc. nous soit accordé. Un ensemble de prérequis sont ainsi indispensables pour opérer des *data centers* en temps de crise. Les *data centers* sont des infrastructures critiques et devraient être reconnus comme tels.

M. Philippe Latombe, rapporteur. Les *data centers* sont-ils reconnus comme des installations critiques dans d'autres pays que la France ? Ou pensez-vous qu'une réglementation européenne devrait être adoptée pour harmoniser les règles à cet égard entre l'ensemble des pays membres ?

M. Olivier Micheli. Il serait en effet intéressant d'approcher cette question à l'échelle européenne. Lors de la première vague de la crise sanitaire, une coordination très forte s'est établie entre les différentes organisations professionnelles, et nous nous sommes rendu compte que la plupart des pays (l'Italie, l'Espagne, l'Angleterre, etc.) avaient très rapidement reconnu aux *data centers* le statut d'installations critiques, pour garantir le fonctionnement de ces bâtiments. Nous n'avons pas réussi à l'obtenir en France. Le gouvernement a signé une lettre de soutien très appuyé au secteur des télécommunications. Nous avons demandé à disposer des mêmes garanties et du même soutien : nous ne l'avons pas obtenu, probablement en raison d'une mauvaise compréhension persistante en France de la nature des *data centers*, de leur impact et de leur criticité.

M. Philippe Latombe, rapporteur. Voulez-vous dire qu'il a manqué au gouvernement et à l'administration une prise de conscience de la nécessité des *data centers*, et de la nécessité d'en permettre le fonctionnement ?

M. Olivier Micheli. C'est exactement ce que je veux dire.

M. Philippe Latombe, rapporteur. Est-ce valable à tous les niveaux, ou le secrétaire d'État au numérique notamment, qui connaît mieux le milieu que certains de ses collègues, s'est-il montré plus réceptif ?

M. Olivier Micheli. Heureusement, nous travaillons extrêmement bien avec la direction générale des entreprises (DGE), qui est à l'écoute, et avec laquelle nous avons eu beaucoup d'échanges et pu travailler sur de très nombreux sujets, notamment relatifs au numérique. La DGE ne travaille cependant pas de manière isolée. Elle a donc fait ce qu'elle a pu. Or, de manière générale, la prise de conscience de l'importance des *data centers* pour le territoire français n'est pas suffisante. Pourtant, la France est un pays d'infrastructures (électriques, de transport, de télécommunications, etc.) dont elle peut être fière. Mais les infrastructures numériques ne sont souvent vues, en France, qu'à travers le prisme des réseaux de télécommunications. Or, ceux-ci ne servent à rien sans *data centers*. C'est un ensemble qui doit fonctionner de manière cohérente. Les réseaux acheminent des données, qui sont stockées dans des *data centers*, puis sont redistribuées. Nous passons donc notre temps à expliquer l'importance des *data centers*, non pas parce que nous travaillons dans ce secteur, mais parce qu'il faut que l'ensemble soit cohérent pour fournir une continuité de service aux citoyens, aux entreprises, aux administrations, etc. Pour l'instant, la prise de conscience n'est pas assez rapide en France. C'est la mission de France Data Center que de l'accélérer, et nous constatons qu'elle est plus rapide dans les autres pays.

M. Philippe Latombe, rapporteur. Ce point est bien noté. Nous examinerons s'il doit être traité au niveau européen ou national.

Y a-t-il d'autres sujets que vous souhaiteriez aborder, et que nous n'aurions pas évoqués ?

M. Olivier Micheli. Quatre marchés principaux, dits « tiers un » (la France, l'Allemagne, l'Angleterre et la Hollande), sont distingués en Europe du reste des marchés, dits « tiers deux ». Si la Hollande (plutôt que l'Espagne ou l'Italie, par exemple) fait partie des marchés « tiers un », c'est parce que l'un des principaux nœuds de télécommunications au monde est historiquement situé à Amsterdam. Un grand nombre de *data centers* se sont donc développés en Hollande, qui vient ainsi de passer devant la France, à la troisième place du classement des pays où se développent le plus de *data centers*. La France y occupe désormais la quatrième place, dont l'Irlande se rapproche très rapidement.

En tant que président de France Data Center et de DATA4, qui constitue une très belle société de *data centers* française, je souhaite vous sensibiliser sur le fait que ces infrastructures sont critiques, attirent de nombreux capitaux, développent des compétences et des savoirs. La France doit donc veiller à ne pas être déclassée de ce point de vue, et s'organiser pour permettre à la filière de se développer encore plus, et de ne pas perdre des parts de marché vis-à-vis d'autres acteurs qui ont compris l'intérêt stratégique de disposer de *data centers* et de données sur leurs territoires, et l'intérêt économique d'attirer ce type d'investissements.

M. Philippe Latombe, rapporteur. Que pourrions-nous faire en termes de formation pour vous aider ? Suffirait-il à court terme de créer quelques filières dans les écoles d'ingénieur, ou faut-il mener un travail à plus long terme ?

M. Olivier Micheli. La formation est toujours un processus long, malheureusement. Il existe en France des filières « télécom », mais pas vraiment de filière *data center*. DATA4 et France Data Center avaient été consultés par l'Université de Rennes, qui envisageait de créer une formation dans les *data centers*. C'était une très bonne idée, qui n'a malheureusement pas abouti à ma connaissance. France Data Center est évidemment disponible pour travailler avec le gouvernement à définir des filières spécialisées dans le *data center*. Une excellente initiative comme « les plombiers du numérique » a commencé dans les réseaux avant de s'étendre aux *data centers*. Elle est désormais partenaire de France Data Center. DATA4 a reçu une vingtaine de jeunes techniciens venus se former aux métiers de base du *data center*. Il ne s'agit pas d'ingénieurs, ni même de techniciens qualifiés, mais cela permet d'aider des jeunes en difficulté et de leur faire découvrir les *data centers*. Des actions, qui vont au-delà de simples expérimentations, sont ainsi lancées et sont très bénéfiques, mais des formations doivent également être créées pour permettre à des ingénieurs et techniciens d'accéder à notre secteur, qui se développe très fortement et a besoin de compétences fortes. La question de la formation est donc très importante.

M. Philippe Latombe, rapporteur. Nous reviendrons vers vous à l'issue de l'ensemble des auditions, mais j'ai bien noté vos suggestions concernant le statut d'infrastructures critiques, les fouilles archéologiques, etc. La question de la stabilité des normes notamment est récurrente, ce qui signifie que votre avis à ce sujet est totalement partagé.

Audition, ouverte à la presse, de Mme Diane Dufoix-Garnier, directrice des affaires publiques, et M. Michel Gesquiere, responsable des ventes d'IBM *(9 mars 2021)*

Présidence de M. Jean-Luc Warsmann, président.

M. le président Jean-Luc Warsmann. Je souhaite la bienvenue aux représentants de la multinationale américaine IBM que nous recevons, Mme Diane Dufoix-Garnier, directrice des affaires publiques d'IBM, MM. Michel Gesquiere et M. Leo Hamon.

Nous avons auditionné plusieurs acteurs du *cloud* au mois de février. Nous recevrons également les représentants de Microsoft, Amazon et Google.

Votre audition s'inscrit dans notre réflexion sur la souveraineté numérique et la façon dont les entreprises technologiques appréhendent cet enjeu. Je suis très heureux, ainsi que mes collègues, de pouvoir échanger avec vous sur la transformation numérique des entreprises, mais aussi de l'État, et sur la manière de conjuguer la protection des intérêts technologiques nationaux et européens avec le développement de nouvelles technologies en Europe.

M. Philippe Latombe, rapporteur. Je souhaiterais solliciter votre avis sur trois sujets.

En tant qu'entreprise privée américaine, spécialisée dans les produits et services informatiques, comment percevez-vous la montée en puissance du thème de la souveraineté numérique dans le débat public, en France, mais aussi en Europe ? Cette problématique se traduit-elle différemment selon vous dans les autres pays où elle se pose ? Comment pouvez-vous participer à sa promotion ou à sa protection, dans un contexte où vous pouvez être soumis au respect de certaines lois extraterritoriales ? Je pense par exemple au *« Clarifying Lawful Overseas Use of Data Act » (Cloud Act)*, mais il en existe d'autres.

Quelles technologies seront critiques dans les prochaines années ? L'entreprise IBM, créée en 1911, s'est fortement diversifiée. Elle offre désormais des produits s'appuyant, par exemple, sur l'intelligence artificielle et la *blockchain*. À l'initiative du gouvernement et des acteurs privés, des initiatives ont été prises en France sur ces segments technologiques cruciaux dans le plan de relance et le programme d'investissements d'avenir (PIA). Comment jugez-vous en conséquence le niveau d'investissement de la France dans ces domaines ? Quels bouleversements technologiques pourraient se produire dans les prochaines années, et sur quelles « technologies de rupture » devrions-nous cibler nos financements ?

Enfin, j'aimerais vous entendre sur le *cloud* et plus généralement sur la transformation numérique des entreprises. Comment jugez-vous l'appétence à se numériser des acteurs publics et privés en France ? Quelles sont les attentes de vos clients dans ce domaine ? Une culture du risque lié aux enjeux de cybersécurité est-elle en train d'émerger face à la nécessité pour les entreprises de recourir massivement au numérique, en période de crise, pour poursuivre leurs activités ?

Mme Diane Dufoix-Garnier, directrice des affaires publiques d'IBM. Je vous remercie de nous accorder cette audition, que nous avons sollicitée et qui nous tient à cœur. Nous travaillons beaucoup et depuis longtemps sur l'objectif de souveraineté numérique, qu'IBM comprend. Nous souhaitons la bâtir et la promouvoir également à notre échelle, dans nos relations avec nos clients, et nous sommes donc prêts à y contribuer, à la hauteur des possibilités d'une entreprise technologique et dans la continuité de notre investissement en Europe.

Vous avez posé de nombreuses questions, toutes très intéressantes. Avant d'y répondre, je souhaiterais vous présenter rapidement IBM. Aujourd'hui, IBM est une entreprise globale, multinationale, présente dans plus de 170 pays, et depuis plus de cent ans en France et en Europe. Du fait de cette histoire, des liens ainsi créés et de la présence territoriale d'IBM en France, la France occupe pour IBM une place stratégique, comme l'Europe en général.

Pour une entreprise technologique, IBM présente en effet la spécificité d'être fortement implantée en région, par exemple à Lille où nous disposons d'un centre de développement de logiciels et d'un centre de cybersécurité. IBM dispose également de centres de recherche et développement (R&D) à divers endroits du territoire, notamment sur l'intelligence artificielle (IA) à Paris-Saclay et à Sophia-Antipolis, d'un centre technologique sur le *cloud computing* à Nice, avec des experts technologiques de ces sujets, et, à Montpellier, d'un centre sur les infrastructures, et, depuis 2018, d'un pôle portant sur les technologies quantiques.

IBM a également tissé des liens importants avec des entreprises emblématiques du tissu économique français, et qui lui font confiance, depuis longtemps, pour se transformer : Orange, la SNCF, le Crédit Mutuel, Michelin et BNP Paribas, par exemple, et certaines font appel à IBM à propos d'enjeux importants comme la traçabilité alimentaire (Carrefour, Labeyrie) ou la santé. Nous travaillons ainsi avec l'ETI Guerbet sur l'aide au diagnostic de cancers du foie et plus récemment de la prostate.

IBM est donc peut-être la plus européenne, ou la plus française, des entreprises multinationales ou des entreprises américaines. C'est ce que nous voulions vous faire appréhender avec ces quelques éléments de présentation.

Notre métier a beaucoup évolué, mais son « fil rouge » a toujours été de concevoir des technologies numériques à la fois performantes et sécurisées, pour aider nos clients à identifier les bons usages et à se transformer, pour être plus compétitifs. Cette philosophie a toujours guidé l'action d'IBM dans son histoire : dans les années 1960, avec la création des grands systèmes et de la disquette ; dans les années 1980, où IBM s'est davantage centrée sur le *BtoC* avec la création des PC ; et jusqu'à nos jours, où nous mettons l'accent sur l'intelligence artificielle ; le *cloud*, que nous développons dans une logique hybride et ouverte (qu'il sera important de présenter à cette mission), avec le rachat en 2018 de Red Hat, un acteur clé de l'*open source* ; et le *Quantum* désormais.

En somme, notre approche vise à permettre à chacun de nos clients d'être souverain technologiquement, à l'échelle de nos relations d'entreprises. En effet, IBM est d'abord, aujourd'hui, une entreprise du *BtoB*, qui a pour seule mission d'aider ses clients à créer de la valeur grâce aux technologies ou à partir de leurs données. Elle a notamment fait le choix stratégique de ne pas entrer en concurrence avec ses clients. La stratégie hybride et ouverte d'IBM dans le *cloud* constitue un autre élément important de la manière dont elle entend aider ses clients à être souverains technologiquement. Cette stratégie fait écho à la doctrine *cloud* définie par l'État en 2018. Une stratégie hybride et ouverte consiste à permettre aux entreprises d'exploiter de façon sécurisée leurs données ou leurs applications, sur différents environnements : en local, sur des *clouds* privés, des *clouds* publics, et des *clouds* multiples, c'est-à-dire incluant des *clouds* IBM, comme d'autres fournisseurs, et ce, de manière totalement interopérable et avec une portabilité des données. Parce que nous pensons que telle est la demande du marché, nous nous sommes engagés dans un axe fort consistant à donner aux entreprises la possibilité de déplacer elles-mêmes leurs données et leurs applications où elles le souhaitent, entre des infrastructures dédiées et mutualisées comme entre différents *cloud providers*, en fonction de leurs contraintes de performance et de sécurité. Avec certains clients, comme BNP Paribas en France, nous allons encore plus loin, en les aidant à construire leur propre solution *cloud* hybride et ouverte, qui intègre donc des éléments privés (qui leur

appartiennent) et les éléments publics que peut apporter IBM grâce à ses investissements R&D dans le *cloud*, y compris public, en conformité avec les exigences de régulation et de souveraineté.

Ceci répond déjà à une partie de vos questions sur la souveraineté. Je continuerai à y répondre, en prenant un peu de distance, pour vous faire part de nos recommandations plus générales à ce sujet, en tant qu'entreprise technologique. Chacun convient que la crise que nous vivons a mis en lumière deux enjeux majeurs de résilience et de souveraineté de nos entreprises. Dans ce cadre, IBM considère le numérique comme une réponse incontournable, dans la mesure où il constitue un vecteur d'agilité et de compétitivité pour les entreprises. Il a d'ailleurs permis à de nombreuses entreprises de continuer à fonctionner durant la crise, et les investissements que nous y consacrons garantissent que les filières actuelles aient un avenir, ce qui constitue un enjeu central de compétitivité, donc de souveraineté, pour la France et l'Europe.

Notre première recommandation à cet égard est de continuer à accélérer la digitalisation des entreprises, donc à mener une politique extrêmement proactive pour renforcer l'offre technologique française et européenne, dans des secteurs stratégiques comme l'IA, le *cloud*, les données, le quantique (qui constitue un champ d'avenir très important, et sur lequel une véritable course internationale est lancée), et bien sûr la cybersécurité. Le secteur des données inclut la *blockchain* et l'Internet des objets *(IOT)*, qui présentent des avantages certains en matière de transparence, de souveraineté et de protection des données.

Si renforcer l'offre technologique est important, il est assez naturel pour IBM, dont c'est le métier, de souligner l'importance d'y associer le développement des cas d'usage. En effet, si les acteurs technologiques développent des technologies sans considération pour les acteurs qui sont en train de se numériser, cela n'aura que peu d'impact. En quantique, par exemple, technologie sur laquelle IBM investit beaucoup, il est tout aussi important, pour la France et l'Europe, de créer les algorithmes de demain, qui, comme cas d'usage, permettront de tirer tous les bénéfices des technologies quantiques, que de construire ces technologies quantiques mêmes. Les deux démarches sont indissociables.

En matière d'investissement technologique, la question des compétences est également extrêmement importante. Je sais que vous l'avez prise en compte. La France dispose à cet égard de nombreux atouts. De nombreux collaborateurs d'IBM France s'impliquent d'ailleurs dans le domaine de la formation, en donnant des cours dans plus de cent établissements d'enseignement supérieur en France. L'investissement dans la formation doit aussi avoir pour objectif que chacun, au-delà des seuls profils de type Bac+5 ou plus, trouve sa place dans la société déjà extrêmement technologique d'aujourd'hui, et qui le sera encore plus demain. Parce que nous considérons qu'il est de notre responsabilité, en tant qu'entreprise, de développer de tels profils, nous travaillons notamment avec le ministère de l'Éducation nationale et d'autres entreprises (BNP Paribas, Orange, La Poste, Salesforce) sur un programme nommé « P-Tech » dans les lycées professionnels.

Notre deuxième recommandation au regard des débats sur la souveraineté numérique française est d'inscrire ces investissements dans une logique d'écosystèmes entre des acteurs publics et privés, et entre des acteurs divers au sein des acteurs privés. Chaque fois qu'il a été possible de renforcer une offre technologique pour en accroître la compétitivité, des écosystèmes forts étaient impliqués, comme c'est le cas à Sophia Antipolis ou à Saclay. La France et l'Union européenne ont donc tout intérêt à promouvoir des partenariats fondés sur des valeurs européennes partagées, avec des partenaires également conscients de l'importance des enjeux de souveraineté, et notamment des enjeux de sécurité et de portabilité, d'interopérabilité et de réversibilité, qui permettent de laisser la maîtrise aux utilisateurs de

leur technologie. C'est ce que nous faisons depuis cent ans, et nous espérons pouvoir continuer ainsi à promouvoir en France une approche « ouverte » de la souveraineté technologique. Par exemple, des investissements publics et privés (notamment d'IBM) ont été annoncés sur les enjeux de transformation IA des entreprises. Avec le soutien de l'État, nous avons lancé en 2020 un projet structurant pour la compétitivité (PSPC), nommé « AIDA », et qui rassemble aux côtés d'IBM une ETI, deux PME et l'Université Paris-Saclay. Notre objectif est de piloter, depuis la France, un projet d'envergure mondiale permettant de positionner la France comme un leader mondial de « l'IA de nouvelle génération », car il s'agit d'un projet de R&D sur une nouvelle vague d'intelligence artificielle.

En dernière recommandation, IBM estime, depuis longtemps, que la souveraineté passe aussi par une forme de régulation, que nous appelons « régulation de précision », visant à cibler de façon proportionnelle les entreprises ou les usages les plus sensibles, quels que soient les secteurs, afin de ne pas freiner la compétitivité et l'innovation dans l'ensemble des usages. IBM soutient à cet égard la proposition d'un Règlement sur les services numériques, le *Digital Services Act (DSA)*, qui régule le type de services proposés, la taille des acteurs, ainsi que leur impact sur la société. IBM fait partie des catégories d'acteurs auxquelles des obligations nouvelles s'imposeront dans ce cadre. La régulation de l'IA constitue un autre enjeu qui fera et fait déjà l'objet de nombreux débats européens. Dans ce domaine, nous sommes également favorables à une régulation ciblée sur les usages à haut risque. Cette approche, portée d'ailleurs entre autres par la France, dans un *non paper* publié en octobre, signifie qu'aucun secteur ne doit être ciblé ou exclu *a priori*, et qu'il ne faut pas réguler la technologie, mais ses usages, en se concentrant sur les plus risqués, grâce à des directives très claires permettant de les définir de manière matricielle.

En conclusion, IBM salue les stratégies de régulation récemment dévoilées par le gouvernement français ou l'Union européenne – la stratégie cybersécurité, la stratégie nationale pour le quantique en France – et les textes et outils qui les accompagnent – les espaces de données communs européens, le *Digital Services Act*, le *Data Governance Act*, etc. Des investissements massifs y sont associés, qu'ils soient publics ou privés. Ils manifestent un effort général.

M. Philippe Latombe, rapporteur. Vous avez commencé par présenter IBM comme une entreprise globale, proposant des *clouds* hybrides. L'extraterritorialité des règles américaines peut paraître en forte contradiction avec l'objectif de souveraineté, puisque IBM est soumis à ces règles, tandis que certains de ses clients pourraient demander que leurs données ne puissent pas partir aux États-Unis. Le *cloud* hybride constitue-t-il pour vous la seule solution pour, à la fois, rassurer ces clients et leur proposer des solutions réellement souveraines ? En tant qu'entreprise IBM, des agences américaines vous ont-elles déjà demandé de leur transférer des données présentes sur des serveurs ou des *clouds* vous appartenant ? Cette menace, qui fait beaucoup parler actuellement, correspond-elle à une réalité ? Nous n'arrivons pas à savoir si des demandes ont réellement eu lieu.

Mme Diane Dufoix-Garnier. Cette question me permettra de préciser la position qui est celle d'IBM France, mais aussi d'IBM US ou Corp. Nous considérons que « Compagnie IBM » (nom officiel de notre société française) est une société française indépendante, opérant en France. Cela signifie qu'IBM France n'est pas soumise à la juridiction d'autorités gouvernementales étrangères qui lui demanderaient de communiquer des données, que ce soit au titre du *Cloud Act* ou de toute autre législation équivalente. Le simple fait qu'IBM France soit la filiale d'un groupe américain amène souvent à penser qu'elle est soumise au droit américain, mais ce fait ne suffit pas à la soumettre au *Cloud Act*, et seul le droit français s'applique en réalité à IBM France, en France, du fait de sa structure juridique. IBM France et

IBM Corp dans son ensemble s'engagent donc très fortement à contester toute demande qui lui serait adressée et qui ne relèverait pas de la compétence des juridictions françaises ou ne serait pas conforme au droit français. IBM France n'est pas une entreprise américaine, et à ce titre n'est pas soumise au droit américain ni aux injonctions de l'administration américaine.

S'agissant de la réalité de cette menace et du nombre de demandes que nous recevons, il faut d'abord rappeler qu'IBM est une entreprise du *BtoB*. Les données de nos clients ne constituent donc pas une priorité pour les demandes gouvernementales, et le *cloud* ne fait pas exception à cet égard. Nous ne recevons donc pas beaucoup de demandes. À ce jour, IBM a reçu extrêmement peu de requêtes dans le cadre du *Cloud Act*. Nous y avons répondu en appliquant scrupuleusement les positions que je vous ai exposées, et plus généralement nos principes en matière de remise des données aux acteurs gouvernementaux, aux agences ou aux juges, et ces positions ont été entendues par le gouvernement américain, puisqu'IBM n'a jamais eu à fournir de données au titre de requêtes *Cloud Act*. Dans les quelques cas où nous avons reçu une telle requête *Cloud Act*, le gouvernement américain a entendu notre approche, et a appelé à la voie de la coopération judiciaire liée au *Mutual Legal Assistance Treaty (MLAT)*. Depuis trois ans, le *Cloud Act* n'a donc eu aucun impact sur l'accès aux données de clients français d'IBM, ou de tout autre client d'IBM situé hors des États-Unis.

Le *cloud* hybride constitue-t-il un rempart supplémentaire par rapport à cette première réponse très juridique, qui constitue une posture de gouvernance concernant notre structuration juridique ? Il fait en effet partie de notre « arsenal » de solutions de protection contre les enjeux de sécurité en général, y compris celui de l'extraterritorialité de certains droits. Nous disposons de solutions technologiques telles que le chiffrement, avec la mise à disposition des clés de chiffrement au client et à lui seul. Selon la sensibilité de ses données, nous pouvons également l'orienter s'il le souhaite, pour le protéger contre le risque d'extraterritorialité des droits, mais aussi contre le risque de cybersécurité en général, vers des solutions comme, par exemple, le *cloud* hybride. Notre premier rempart, et le plus important pour nous, reste cependant notre posture juridique et de gouvernance.

M. Philippe Latombe, rapporteur. Votre position, selon laquelle IBM France est soumise au droit français et n'est donc pas soumise au *Cloud Act*, n'est pas partagée par certains juristes, au motif notamment qu'un conflit entre Microsoft et les États-Unis à ce sujet n'est toujours pas réglé depuis 2013. Une demande d'information avait en effet été transmise à Microsoft Irlande, qui était de droit européen et communautaire, comme aujourd'hui IBM France. Ce conflit a désormais été renvoyé aux cours inférieures depuis la publication du *Cloud Act*. Par ailleurs, le *Cloud Act* s'applique aux entités juridiques, mais aussi aux serveurs. Pouvez-vous certifier à vos clients en France qu'IBM n'utilise aucun serveur d'une autre filiale ou entité du groupe IBM, qui, elle, serait soumise au *Cloud Act* sans pouvoir répondre qu'elle constitue une société française ? Garantissez-vous une étanchéité totale dans vos serveurs et dans la gestion de leurs données, que ce soit en matière de contrôle, de sécurité, de redondance, etc. ?

Mme Diane Dufoix-Garnier. La position d'IBM est en effet différente de celle d'autres grands acteurs internationaux, dont je ne connais cependant pas la structure juridique propre. IBM Corp considère que le droit des sociétés doit être pris en compte, et que la manière dont nous avons construit nos filiales en fait des entités juridiques absolument distinctes. Nos contrats et nos relations avec nos clients sont en effet construits de telle sorte que les filiales étrangères d'IBM Corp (y compris donc la filiale française) n'ont aucune activité commerciale aux États-Unis qui justifierait une applicabilité du *Cloud Act*. Et nous contestons l'idée, effectivement partagée par certains juristes, selon laquelle un simple lien en capital entre IBM US et une filiale étrangère d'IBM soumet cette dernière à la compétence légale des États-Unis.

Dans les rares cas où cette position a dû être testée, elle a été entendue par la puissance qui a instauré le *Cloud Act* aux États-Unis.

Notre approche inclut toutefois plusieurs autres remparts. Bien avant le *Cloud Act*, IBM avait décidé de contester par tout moyen toute demande émise directement auprès d'IBM US qui ne suivrait pas les voies légales reconnues sur le plan international. Les principaux arguments que nous engagerions à cet égard consisteraient à indiquer que la demande concerne des données sous contrôle de la filiale française, qui n'est pas soumise au droit américain ; et que ces données ne sont pas en possession, sous la garde ou sous le contrôle d'IBM US, même si celle-ci est soumise à la compétence personnelle de l'État à l'origine de la demande. Cette posture est donc forte, et différente de celle d'autres acteurs, mais nous l'avons testée, et nous l'avions adoptée dès 2014, donc bien avant le *Cloud Act*. Toutes les entreprises du monde ont l'occasion de contester les injonctions d'un juge. Cela n'a rien de tabou aux États-Unis, et, selon le contexte, IBM utilisera tous les moyens disponibles en droit à cette fin.

M. Philippe Latombe, rapporteur. Le fait d'utiliser un produit construit d'abord aux États-Unis, comme Watson, ne constitue-t-il pas un lien qui permettrait juridiquement aux agences américaines de vous demander de transmettre les données collectées ou traitées par cet outil, qui, lui, a été créé aux États-Unis et est employé commercialement en France ? Ou bien avez-vous prévu un système de licence entre IBM Corp et IBM France, et alors comment fonctionne-t-il ? Qu'avez-vous prévu s'agissant de ce type d'innovations en matière d'intelligence artificielle, ou d'algorithmes que vous pourriez développer aux États-Unis et ensuite utiliser dans chacune de vos filiales à l'avenir ?

Mme Diane Dufoix-Garnier. Je comprends votre question, mais j'en reviens au fait que, par construction, IBM France est soumise au droit local, en raison de la manière dont nous avons construit nos relations commerciales en France avec nos clients. Même dans le cas où un lien existerait avec les États-Unis, notre posture de gouvernance, telle qu'elle est inscrite y compris dans nos contrats, consiste à affirmer qu'IBM US contestera par tout moyen une demande qui concernerait les données d'un client français, notamment. Des allers-retours juridiques pourraient être initiés par une demande qui nous serait adressée aux États-Unis, mais la filière française serait fondée à répondre que, par nature, en tant que société française ne pratiquant pas de business aux États-Unis, elle n'est pas soumise au *Cloud Act* ni à l'extraterritorialité de ce droit, quelles que soient ses interactions avec des solutions développées par IBM aux États-Unis.

M. Philippe Latombe, rapporteur. J'entends votre position, mais ce n'est pas la position aujourd'hui dominante parmi les juristes, notamment suite à l'invalidation du *Privacy Shield* par l'arrêt *Schrems* II. Nous aurons l'occasion, au cours de nos auditions ultérieures, comme en considération des audiences en cours devant le Conseil d'État et ailleurs, de faire le point à ce sujet.

Mme Diane Dufoix-Garnier. Dans le cas de *Schrems* II, l'arrêt de la Cour portait sur une question de transfert de données, et non sur une question d'extraterritorialité. Il a confirmé, en les assortissant de mesures renforcées, la validité des clauses contractuelles-types qu'IBM a toujours utilisées comme cadre principal pour le transfert des données, avec des mesures renforcées de protection que nous appliquons depuis des dizaines d'années. Suite à l'arrêt *Schrems* II, nous sommes allés encore plus loin en incorporant directement dans nos contrats notre politique d'engagement à contester toute demande qui ne passerait pas par notre client, mais serait réalisée hors des voies juridiques internationalement reconnues.

M. Philippe Latombe, rapporteur. Parmi les technologies d'avenir figurent pour vous l'intelligence artificielle et le quantique. Quel est l'avenir à moyen terme de ces

technologies, pour lesquelles vous avez installé des centres de recherche en France ? À quoi serviront-elles dans la vie des entreprises ? Faut-il directement tourner les entreprises vers ces technologies, ou continuer à les numériser en conformité avec l'état de l'art actuel ?

Mme Diane Dufoix-Garnier. L'avenir de ces technologies tient à l'usage qui en sera fait par nos clients pour renforcer leur compétitivité. Comme je l'ai indiqué s'agissant du quantique, une technologie n'a pas d'intérêt si elle n'offre pas un usage pour l'industrie de demain, la santé de demain, les villes intelligentes, etc. Il existe un enjeu pour la France à se positionner à la pointe de ces technologies dans leur dimension « offre » : sur ce plan, il s'agit d'investir en R&D et de développer les compétences. Nous recommandons une logique d'écosystème, car certains acteurs ont, de manière privée, beaucoup investi dans ces technologies, et peuvent donc procéder à des transferts technologiques de savoir-faire. Cet enjeu est absolument fondamental. Avec le Crédit Mutuel, nous avons réuni une équipe commune en intelligence artificielle, avec une vingtaine d'experts d'IBM et une vingtaine du Crédit Mutuel qui développent ensemble l'IA du Crédit Mutuel. Des usages sont ainsi développés dans un travail en écosystème. Un enjeu de cas d'usage nous paraît fondamental, au-delà de l'investissement en R&D dans l'offre technologique elle-même.

Une question de compétences se pose également. Le quantique constitue un champ entier, qui n'en est encore qu'à ses prémices, même si les progrès sont rapides. À côté de l'investissement dans cette technologie (dans les ordinateurs, les simulateurs, etc.), l'enjeu est de constituer dès aujourd'hui des écosystèmes, par exemple avec de grandes entreprises françaises et des universités, pour développer les algorithmes quantiques qui seront probablement au centre des usages de demain.

M. Michel Gesquiere, responsable des ventes d'IBM. Notre stratégie pour les années à venir repose également sur le *cloud* hybride, qui est censé combiner « le meilleur des deux mondes ». En fonction de la criticité des applications concernées, qui est très différente dans le domaine industriel, bancaire ou des biens de grande consommation, il s'agit de permettre à nos clients de choisir de localiser leurs applications ou leurs données dans des environnements privés (plus protecteurs) ou dans des environnements publics, où il est possible de bénéficier de trois effets à l'impact économique extrêmement important :

– une économie d'échelle et une automatisation très importante ;

– l'innovation dans le monde ouvert des logiciels : en rachetant Red Hat, IBM s'est ainsi dotée d'une offre tirant parti de cette innovation dans le domaine du *cloud* ;

– et un mode économique consistant à disposer d'une puissance informatique ou d'une puissance de stockage basée sur la vente d'un service avec la flexibilité adéquate.

Cette stratégie nous paraît structurante pour les années à venir. Toutefois, deux évolutions technologiques devront s'y ajouter.

Nous pensons ainsi que le *Quantum* peut être adapté à certaines situations, certains algorithmes ou certains problèmes très particuliers. Par exemple, les algorithmes qu'il permettra de développer seront très adaptés à certains des problèmes d'optimisation qui se posent en finance et en logistique.

Le champ d'application de l'intelligence artificielle s'accroîtra considérablement également dans les années à venir. Elle a déjà été déployée dans le domaine de l'expérience « client ». Elle servira aussi d'assistant pour accroître la performance des employés : c'est en ce sens qu'elle est envisagée dans notre partenariat avec le Crédit Mutuel. L'automatisation

des processus industriels passera également par l'intelligence artificielle. Avec l'IOT et la 5G, le nombre des données s'accroîtra et l'intelligence artificielle permettra de les transformer en éléments de compétitivité et d'automatisation des performances.

Certains problèmes trouveront donc une solution dans le *Quantum*, mais l'ensemble de la stratégie technologique d'IBM sera centré sur le *cloud* hybride, pour combiner à la fois la protection des données critiques dans certains secteurs et l'effet d'échelle ou d'automatisation qu'apportent les stratégies publiques.

M. Philippe Latombe, rapporteur. Pensez-vous que les collectivités, et les collectivités territoriales notamment, sont encore loin d'avoir atteint le niveau de numérisation qui devrait être le leur, et pensez-vous qu'elles ont intégré la notion de cybersécurité dans cette numérisation ? Au-delà des grands groupes, qui l'ont peut-être déjà intégré, cet enjeu est-il suffisamment prégnant dans les PME, les ETI et les collectivités territoriales ? Presque toutes les collectivités territoriales souhaitent aujourd'hui développer des *smart cities*. Ont-elles intégré la cybersécurité dans ce domaine, ou revient-il précisément aux acteurs privés, tels que vous, de leur en rappeler la nécessité ?

M. Michel Gesquiere. Nous pensons qu'une prise de conscience a eu lieu, mais qu'il reste beaucoup d'actions à mettre en œuvre. Dans le domaine du *cloud*, les sources décentralisées vont se développer de plus en plus, avec *l'Edge computing*, l'IOT et la 5G. Comme vous l'avez dit, les ETI ne disposent pas à cet égard des mêmes moyens que les grands groupes. Sur le marché de la cybersécurité, une accélération des investissements est prévue, en raison de l'accélération des menaces, mais aussi d'une plus grande fragilité du réseau des petites et moyennes entreprises, en raison des interconnexions croissantes dans les chaînes de valeur sous l'effet de la globalisation. Ce sujet est donc essentiel, et nous nous efforcerons d'accompagner les entreprises dans cet effort et les investissements qui seront indispensables à cet égard.

M. Philippe Latombe, rapporteur. Comment aborderez-vous ce marché ? Intégrerez-vous des solutions de cybersécurité à l'intérieur des produits que vous proposerez, ou sous-traiterez-vous à des sociétés spécialisées différents types de réponses à des menaces cyber, en utilisant des logiciels que vous rendrez interopérables avec vos propres systèmes ?

M. Michel Gesquiere. IBM propose à la fois des offres logicielles et des services permettant de les intégrer. En même temps, nous restons très humbles. Même si nous disposons d'une position forte, reconnue et historique dans le domaine de la cybersécurité, nous ne pouvons pas revendiquer d'avoir à notre disposition l'ensemble des solutions. Nous proposons donc les solutions logicielles dont nous disposons, et nous les intégrons, mais nous ouvrons aussi sur d'autres éditeurs, qui fournissent d'autres solutions logicielles, en particulier sur des sujets « de niche » très précis, et nous proposons à nos entreprises de les aider à les intégrer. Nous pensons ainsi que l'avenir est à l'intégration de solutions, qui peuvent être des solutions IBM ou non, l'important étant de disposer des services et de la gouvernance qui permettront d'intégrer l'ensemble.

Mme Diane Dufoix-Garnier. Nous faisons partie de la *Charter of Trust*, qui a été lancée par Siemens, Total ou Atos avec IBM, s'agissant des acteurs français. Conscients que personne ne résoudra seul le problème de la cybersécurité, nous cherchons à y mettre en place des bonnes pratiques ou des solutions permettant très concrètement d'augmenter notre niveau de compréhension de ces enjeux, et nos capacités de réaction. L'un des principes de cette *Charter of Trust*, sur lequel nous avons travaillé, est celui de la responsabilité à travers la chaîne de sous-traitance. Nous avons essayé de formaliser des principes et des standards très

simples, accessibles y compris à une PME qui pourrait intervenir en sous-traitance d'un grand groupe, afin que chacun soit conscient des objectifs à atteindre.

M. Philippe Latombe, rapporteur. Ressentez-vous aujourd'hui des menaces plus prégnantes et d'un niveau supérieur à ce qu'il était précédemment ? Les hôpitaux ont subi des attaques récemment. Deviennent-elles plus sophistiquées et plus fréquentes ? Disposez-vous de moyens pour identifier leur origine ? La question s'est notamment posée de savoir si les attaques récentes sur Microsoft Exchange venaient d'un pays ou seulement de groupes souhaitant gagner de l'argent. La géopolitique impacte-t-elle la cybersécurité, et comment l'intégrer alors dans les systèmes critiques dont vous devez disposer en tant que fournisseur de solutions pour des banques, de grandes entreprises, des collectivités ou l'État ?

M. Michel Gesquiere. Les études réalisées montrent indéniablement que le nombre des attaques a augmenté en France et en Europe sur les douze derniers mois glissants.

Par ailleurs, les questions de cybersécurité rejoignent selon nous l'enjeu du *cloud* hybride. Plus les gouvernances répartissent adéquatement les applications et les données entre des environnements privés ou publics, plus les moyens existent, au-delà des seules techniques de protection, pour sécuriser les applications ou les données les plus critiques. C'est très vrai dans le secteur privé, et c'est probablement la raison pour laquelle la plus grande banque française et européenne, la BNP, s'appuie sur IBM pour développer sa propre solution, avec un niveau de sécurité extrêmement élevé.

Mme Diane Dufoix-Garnier. La menace est effectivement multiforme. Elle provient de nombreuses sources. Le partage d'intelligence et la coopération entre les acteurs, y compris publics, de la cybersécurité est essentielle à cet égard, et pour progresser en matière de détection. Notre centre de cybersécurité à Lille compte des experts qui travaillent à permettre de détecter une menace le plus tôt possible lorsqu'elle émerge, car on sait qu'il sera alors possible d'y réagir plus rapidement. Le campus Cybersécurité qui sera lancé constitue à cet égard une initiative française extrêmement intéressante, car personne ne sera en mesure de résoudre ce problème seul. Toutes les logiques d'écosystème comme celle-ci sont donc à encourager absolument.

M. Philippe Latombe, rapporteur. Souhaiteriez-vous évoquer d'autres points sur ces questions de souveraineté européenne et française ?

Mme Diane Dufoix-Garnier. Nous aurions simplement pu vous parler davantage de notre initiative P-Tech de développement des compétences, qui fait appel à des profils différents de ceux auxquels recourt traditionnellement notre industrie. Faire connaître cette initiative, qui est en cours de déploiement avec le ministère de l'Éducation nationale, serait très intéressant notamment pour convaincre d'autres entreprises de l'intérêt de s'associer à quelques lycées professionnels pour faire progresser l'inclusion par le numérique, qui constitue un enjeu important et enthousiasmant. Nous nous permettrons donc de vous adresser des éléments écrits à ce sujet.

M. Philippe Latombe, rapporteur. Nous les recevrons avec plaisir, d'autant que nous ouvrirons une séquence de nos auditions relatives à l'éducation dans les semaines à venir.

M. Michel Gesquiere. Nous avons beaucoup parlé de technologie, mais nous pensons vraiment que c'est son usage qui permettra aux États ou aux entreprises d'acquérir un avantage concurrentiel. Plus les technologies utilisées seront sophistiquées, comme l'intelligence artificielle, plus nous aurons besoin de différentes formes d'intelligences : il faudra des intelligences très cognitives pour concevoir les solutions, mais aussi des intelligences très

pratiques pour penser les usages et l'insertion de ces solutions dans le corps social des entreprises. À cet égard, l'initiative P-Tech a un rôle essentiel à jouer, non seulement en faveur de l'inclusion, mais aussi d'une plus grande efficacité, en permettant de trouver le bon usage et la bonne intégration de ces solutions sophistiquées au sein des entreprises. Entre la performance, la compétence et les différentes formes d'intelligence, un lien existe, qui est absolument clé.

Audition, ouverte à la presse, de M. Claude Gissot, inspecteur général de l'INSEE, directeur de la stratégie, des études et des statistiques (DSES), et de Mme Stéphanie Naux, directrice de mission au cabinet du directeur de la stratégie, des études et des statistiques, de la caisse nationale d'assurance maladie (CNAM)

(9 mars 2021)

Présidence de M. Philippe Latombe, rapporteur.

M. Philippe Latombe, rapporteur. Nous poursuivons notre cycle d'auditions consacrées au numérique en santé, en auditionnant aujourd'hui M. Claude Gissot, directeur de la stratégie, des études et des statistiques (DSES), et de Mme Stéphanie Naux, directrice de mission au cabinet du directeur de la stratégie, des études et des statistiques de la caisse nationale d'assurance maladie (CNAM).

Au cours des dernières semaines, nous avons déjà entendu à ce sujet la délégation ministérielle du numérique en santé, l'Assistance publique – Hôpitaux de Paris (AP-HP), ainsi que les représentants du Health Data Hub.

La CNAM est un établissement public national à caractère administratif (EPA), qui constitue la tête de réseau opérationnelle du régime d'assurance maladie obligatoire en France. Elle est placée sous la double tutelle du ministère des Solidarités et de la santé et du ministère de l'Économie, des finances et de la relance. Elle est en charge du système national des données de santé (SNDS), qui rassemble un certain nombre de bases de données de santé à des fins de recherche. La CNAM est donc particulièrement concernée par les enjeux de protection des données de santé, et de soutien à la recherche et à l'innovation. À ce sujet, nous aurons l'occasion de revenir sur le refus du conseil de la CNAM de transférer une copie des données du SNDS au Health Data Hub, dès lors qu'il utilisait la solution de *cloud* Azure de Microsoft.

Pourriez-vous compléter cette présentation en expliquant notamment le rôle de la CNAM en matière de numérisation de notre système de santé ? Comme cela nous a été rappelé la semaine dernière, de nombreux acteurs interviennent dans ce domaine, qu'il s'agisse des agences régionales de santé (ARS) ou des centres hospitaliers, la stratégie « Ma santé 2022 » étant pilotée par la délégation ministérielle du numérique en santé. Comment la CNAM participe-t-elle à cette dynamique ? La notion de souveraineté numérique est-elle prise en compte dans vos actions ?

En second lieu, pourriez-vous présenter la base de données que constitue le SNDS, en précisant ses différentes composantes et en détaillant son fonctionnement ? Quels choix techniques ont été effectués et quels types de données sont rassemblées en son sein ? Cet échange nous permettra d'évoquer ensuite les raisons du refus récent du conseil de la CNAM de transférer auprès du Health Data Hub une copie des données du SNDS, et les évolutions envisageables à terme sur cette question.

Enfin, je souhaiterais évoquer avec vous l'enjeu de la protection des données de santé et des systèmes d'information de l'assurance maladie. L'actualité récente a été marquée par des attaques cyber, très médiatisées, contre des établissements de santé, avec une fuite de données record qui concernerait environ 500 000 patients. Comment appréhendez-vous cet enjeu ? Échangez-vous avec l'agence nationale de la sécurité des systèmes d'information (ANSSI) sur cette question ? La sécurité constitue en effet une condition indispensable pour

rassurer les citoyens et leur montrer l'apport du numérique en santé. À ce sujet, nous sommes naturellement intéressés par votre regard sur les meilleurs voies et moyens permettant d'inclure les citoyens dans cette transformation.

M. Claude Gissot, directeur de la stratégie, des études et des statistiques (DSES) de la caisse nationale d'assurance maladie. La CNAM est un EPA, mais surtout le principal assureur obligatoire en santé. Il couvre maintenant presque la totalité de la population résidant en France, ou ayant du moins ouvert des droits en France auprès de l'assurance maladie. Son activité historique de paiement des prestations de santé aux assurés et de remboursement des soins aux professionnels ou aux assurés s'est élargie fortement ces dernières années à l'accompagnement des patients pour la gestion de leurs droits ou de leurs risques en matière de santé. Nous avons également développé une activité très forte au titre des relations conventionnelles avec les professionnels, notamment libéraux, puisque leur activité est régie par une convention négociée entre les représentations professionnelles de libéraux et l'assurance maladie, soit principalement la CNAM. Bien entendu, nous travaillons aussi à l'amélioration de la qualité des soins et surtout de l'efficience des processus de soin, puisque l'objectif général de la CNAM est de garantir que le système de solidarité en santé existant aujourd'hui en France soit pérenne et résiste aux évolutions de la santé, dont nous pourrons si vous le voulez préciser les facteurs très puissants existant aujourd'hui.

Dans son activité, la CNAM a développé beaucoup de services numériques auprès des professionnels de santé ou des assurés, principalement avec le compte AMELI de l'assurance maladie que les assurés peuvent ouvrir, mais qui a été complété, il y a quelques années, par le dossier médical partagé (DMP), que la CNAM a repris pour assurer son développement. Presque 10 millions de DMP ont ainsi été ouverts aujourd'hui et complétés par l'assurance maladie elle-même, ce qui a permis de lever les difficultés des versions précédentes du DMP. La CNAM a également développé des services auprès des professionnels de santé, en lien avec la digitalisation de la pratique professionnelle, en termes de remboursement, avec les feuilles de soin électroniques, qui existent depuis longtemps, mais aussi des téléservices pour les prescriptions d'arrêt de travail, les déclarations de médecin traitant, etc. Tous ces outils sont développés depuis plusieurs années par la CNAM dans un objectif de numérisation de l'activité de gestion de la santé, porteuse d'efficacité pour les professionnels de santé et les assurés, mais aussi pour la CNAM.

Par ailleurs, nous collectons depuis longtemps des données « médico-administratives » (correspondant en réalité aux remboursements des soins de ville et hospitaliers) dans une base nationale décisionnelle qui s'appelait initialement, et s'appelle toujours, le Système national d'information interrégime de l'assurance maladie (SNIIRAM), qui constitue probablement la base principale du SNDS actuellement. Cette base consolide ainsi les remboursements des soins de ville et hospitaliers de tous les assurés, quel que soit donc leur régime, et sur un historique long, puisque le SNIIRAM a été créé à la fin des années 1990, c'est-à-dire en 2000 sur une enveloppe de financement de 1998-1999. Le temps que la quantité d'information considérable ainsi réunie soit organisée, le SNIIRAM est opérationnel de manière totalement efficace et exhaustive depuis les années 2005-2006. Les premières exploitations réellement fortes qui en ont été faites datent de 2007. Dès le départ, ce système d'information a été ouvert à l'ensemble des acteurs de la santé, d'abord aux acteurs publics, et, évidemment, à tous les acteurs de la recherche, même s'il a fallu un certain temps pour que les chercheurs s'intéressent à ces données administratives, qui ne comportent pas de données médicales au sens de diagnostics ou de résultats en termes de santé, ce qui peut parfois en détourner les chercheurs cliniciens. Néanmoins, nous avons pu démontrer, et l'assurance maladie notamment en les utilisant, que ces données étaient très utiles pour analyser le système de santé et le système de soins, afin d'en déduire des informations sur la qualité des soins, l'efficience, etc. À partir de

2019, le SNIIRAM a été élargi pour être transformé en SNDS en incluant d'autres sources de données, c'est-à-dire principalement les causes de décès et prochainement les données des maisons départementales des personnes handicapées.

La CNAM a donc évidemment été un membre historique de l'Institut des données de santé (IDS), créé en 2002 pour regrouper les acteurs de la santé autour de la recherche d'une meilleure utilisation des données de la santé et de leur ouverture à l'ensemble des acteurs de la santé. Les seules bases de données médico-administratives existantes à l'époque étaient le SNIIRAM et le programme de médicalisation des systèmes d'information (PMSI), qui relève tous les séjours hospitaliers réalisés dans les établissements de santé publics comme privés, et dans tous les secteurs. La CNAM a ainsi poursuivi son rôle de recueil et de mise à disposition des données à l'ensemble des acteurs de santé dans le cadre de l'IDS, devenu Institut national des données de santé (INDS) en 2016, et maintenant avec le Health Data Hub (HDH) depuis la loi de 2019. La CNAM conserve aujourd'hui ce rôle à travers son portail. Elle est un membre du groupement d'intérêt public (GIP) HDH. À ce titre, elle participe aux différentes instances de régulation du pilotage du HDH, comme tous les acteurs de santé, qui sont tous présents dans l'assemblée générale du HDH. Le vice-président du HDH notamment est un représentant de France Assos Santé, et il y représente donc les patients.

Historiquement, la CNAM a mis en place le SNIIRAM, qui constitue encore aujourd'hui la base de données principale du système de soins français. Nous sommes également le partenaire principal du HDH, aujourd'hui, pour sa constitution, sa montée en charge et sa montée en compétences, notamment s'agissant de l'utilisation de ses données dans sa « base centrale » qui rassemble le SNIIRAM, la base des causes de décès et le PMSI. En effet, les projets d'études déposés aujourd'hui sont principalement réalisés sur le portail de la CNAM, et principalement accompagnés par les équipes de la CNAM. Nous travaillons de manière très rapprochée avec le HDH pour partager notre expérience sur les données, sur la réalisation des projets, les appariements, etc. De manière générale, la CNAM apporte donc son soutien, et toute son expertise, au projet du Health Data Hub, car il doit permettre une plus grande utilisation des données, un enrichissement des données médico-administratives par des données plus médicalisées, incluant notamment des données cliniques, qui pourront décupler les possibilités d'analyse et d'étude afin de contribuer, au final, à l'amélioration des prises en charge des patients.

Mme Stéphanie Naux, directrice de mission au cabinet du directeur de la stratégie, des études et des statistiques (DSES) de la caisse nationale d'assurance maladie. Au moment de sa création en 2016, le système national des données de santé (SNDS) s'inscrivait dans la continuité du SNIIRAM, qu'il élargissait.

Créé au début des années 2000, le SNIIRAM visait à constituer une base d'information exhaustive sur le recours aux soins, avec un historique long (jusqu'à vingt ans), pour suivre non seulement les dépenses, mais aussi les parcours de soin, les effets à long terme des prises en charge et des pathologies traitées, ce qui a constitué son premier intérêt pour la recherche. Les données de cette base sont principalement issues de systèmes de gestion initialement utilisés à d'autres finalités : en particulier le remboursement des soins, la rémunération des producteurs de soins, les référentiels associés. Le SNIIRAM comprend les données de ville produites par l'assurance maladie (c'est-à-dire l'ensemble des informations issues des feuilles de soins), auxquelles sont associées les données des séjours hospitaliers issues du PMSI. Toutes ces données sont « pseudonymisées », ce qui signifie que toutes les données directement identifiantes sont supprimées : aucun nom, aucun prénom, aucune adresse précise ne sont conservés, et le numéro de sécurité sociale ou NIR (numéro d'inscription au répertoire de l'INSEE) est remplacé par un pseudonyme irréversible, qui est constitué par un hachage,

mais qui est unique pour une même personne, ce qui permet peu à peu d'articuler les données entre elles. La base est ainsi construite par l'attribution dans le temps des mêmes données aux mêmes personnes.

En 2016, la première version du SNDS a donc ajouté au périmètre initial du SNIIRAM les données des maisons départementales des personnes handicapées (MDPH), qui sont gérées et produites par la Caisse nationale de solidarité pour l'autonomie (CNSA), et les données des causes de décès incluses à la base du centre d'épidémiologie sur les causes médicales de décès (CépiDC) produite par l'Inserm. Ces données ont été ajoutées à la base du SNIIRAM avec un chaînage direct et une association physique des données sous le même pseudonyme, pour être réunies au sein du portail de la CNAM.

Une étape supplémentaire a été franchie en 2019 à l'occasion de la loi relative à l'organisation et à la transformation du système de santé (OTSS), qui a complété largement le cadre du SNDS en ouvrant, à côté de cette base, désormais nommée « principale » ou « historique », un catalogue de bases de données ayant vocation à être appariées ou appariables avec les données de la base principale, et qui sont pour beaucoup des données destinées aux professionnels de santé : données de résultats et d'imagerie, mais aussi d'autres sources.

La loi de 2019 a également créé le Health Data Hub, ou Plateforme des données de santé. Il s'agissait d'abord d'élargir les missions auparavant confiées à l'INDS :

– d'une part, des missions liées à la gestion du guichet unique de dépôt des dossiers de demande d'accès aux données, donc à l'initiation du circuit d'accès aux données par le comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé (CESREES) et la Commission nationale de l'informatique et des libertés (CNIL) ;

– d'autre part, une mission de constitution de lieux d'échanges entre les acteurs, producteurs et utilisateurs des données. Depuis 2019, la plateforme de données de santé Health Data Hub a, comme la CNAM, une mission de mise à disposition des données aux acteurs souhaitant les utiliser, donc la constitution d'une plateforme pour la mise à disposition de ces données. HDH est également en charge de la constitution du catalogue des données et doit promouvoir le partage et l'usage de ces données, ainsi que la recherche et l'innovation en santé et l'information des usagers.

Deux voies d'accès aux données du SNDS existent.

La première voie est celle des « accès permanents », qui existent depuis 2016 pour les institutions remplissant une mission de service public (directions centrales des ministères, agences de santé, instituts de recherche comme l'Inserm ou l'INDS). Celles-ci disposent d'un accès direct aux données sur le portail de la CNAM, selon un périmètre défini par décret pour chaque institution, en fonction de ses missions, de zones géographiques, d'historiques de données et de son accès plus ou moins détaillé à certaines bases. Cet accès permanent est ouvert depuis la première version du SNDS, sur le portail de la CNAM. Chaque institution disposant d'un accès permanent peut également habiliter des acteurs individuels à travailler sur ces données.

La deuxième voie est celle des « accès sur projet », qui existent pour toutes les institutions ou entreprises qui, soit ne disposent pas d'un accès permanent et souhaitent développer un projet spécifique, soit disposent d'un accès permanent, mais souhaitent en élargir le périmètre pour un projet ou une étude donnée. Les porteurs de projet doivent alors déposer les demandes d'autorisation selon un protocole détaillant leur étude auprès du guichet unique ou du secrétariat du HDH. Ces protocoles sont examinés par le CESREES, qui rend un

avis avant transmission pour autorisation ou non par la CNIL. Celle-ci peut aussi autoriser une mise en œuvre sur des « bulles sécurisées », prévues spécifiquement par la CNIL, pour accueillir certains projets.

M. Claude Gissot. Pour la CNAM, en tant que producteur et utilisateur de données jouant un rôle de régulateur du système de santé, la souveraineté numérique permet surtout une exploitation la plus efficace possible des données pour alimenter la recherche, la santé publique et l'innovation, sans que les innovations en santé en France dépendent de pays qui construiraient des bases de données à même de porter des projets scientifiques et technologiques, mais aussi de les assurer. Il n'est pas certain en effet que le cadre organisationnel propre à la France permettrait de produire les mêmes résultats en utilisant des données produites dans d'autres pays et d'autres contextes.

S'agissant du partage des données de santé et des freins éventuels existant à cet égard, il faut d'abord souligner que le SNIIRAM et le SNDS ont déjà été très utilisés. Ils permettent la réalisation de 150 projets d'études par an par des opérateurs publics ou privés, et le *benchmark* présenté par le Health Data Hub, il y a quelques semaines, lors de son assemblée générale montre que le nombre de projets ainsi conduits n'est pas tellement supérieur, dans d'autres pays, même si les contenus des bases de données exploitées ne sont pas nécessairement comparables. Certaines des bases de données étrangères sont moins larges en nombre, mais contiennent davantage de données médicalisées, ce qui leur donne des potentiels différents. L'avantage du SNDS est toutefois d'être exhaustif quant à la population, ce qui lui confère une puissance statistique sans égal pour les études qu'il est censé rendre possibles.

Ces projets peuvent être menés par des opérateurs publics ou privés, mais ils ne peuvent évidemment pas utiliser ces données pour des finalités interdites par la loi, comme la modification des contrats d'assurance individuels et la promotion des produits de santé auprès des professionnels. Les projets qu'ils présentent doivent donc pouvoir exclure ces finalités.

Par ailleurs, le SNIIRAM-SNDS contient des données administratives, recueillies à des fins premières de gestion, et non d'étude. L'exhaustivité et la précision de ces données (qui incluent le code CIP des médicaments et le codage précis des actes réalisés) permettent d'analyser les systèmes de recours aux soins avec une grande efficacité. Néanmoins, ces données ne sont pas construites initialement pour des finalités d'étude, et leur réutilisation dans ce cadre requiert une expérience et une formation importantes. C'est pourquoi la CNAM accompagne, depuis dix ans maintenant, des centaines de chercheurs afin qu'ils puissent réaliser leurs études. Elle a récemment publié un article dans la Revue française de santé publique dressant le bilan de l'utilisation de ces bases de données, et montrant notamment qu'un nombre extrêmement important d'études recourant à ces données ont été référencées dans des revues à comité de lecture, ce qui en montre le succès.

Le SNIIRAM-SNDS contient toutefois assez peu de données médicales : les résultats des tests, les stades des cancers, etc. n'y sont pas fournis. Son potentiel vient donc essentiellement des registres et des cohortes qui sont organisés par ailleurs par de nombreuses unités de recherche, et qui sont malheureusement encore assez insuffisamment utilisés, notamment en appariement avec le SNIIRAM, alors que ces données sont extrêmement complémentaires. En effet, les entrées des cohortes et des registres passent par des pathologies très précises, auxquelles le SNIIRAM-SNDS pourra associer très précisément l'ensemble des comorbidités auxquelles les patients sont soumis également, en permettant ainsi de comprendre leur parcours de soins au-delà de la seule pathologie concernée par la cohorte ou le registre.

M. Philippe Latombe, rapporteur. La semaine dernière, nous avons interrogé l'Assistance publique- Hôpitaux de Paris (AP-HP). Elle s'est dite très intéressée par les données du SNIIRAM-SNDS, mais a confié avoir beaucoup de mal à y accéder, du fait notamment de la complexité de la procédure de dépôt des projets auprès de la CNIL. Tout le monde est donc aujourd'hui d'accord avec vous pour dire qu'il s'agit de données très intéressantes. Avec l'appariement des cohortes, elles permettraient en effet de disposer d'une vision très large de la situation. Toutefois, il semble difficile d'y accéder. Existe-t-il un moyen de fluidifier ou de simplifier l'accès aux données du SNDS ?

M. Claude Gissot. Nous partageons naturellement cette problématique du fait de notre expérience de l'accès aux données depuis de nombreuses années, et notamment au sein du HDH.

Le parcours d'accès à ces données a été défini par la loi. Il encadre la manière dont les dossiers doivent être déposés auprès du CESREES, qui les examine, au regard de leur intérêt public, de leur méthodologie et de la pertinence de la recherche envisagée, etc. Il émet un avis, qui est transmis à la CNIL, laquelle fournit sa réponse.

Plusieurs questions se posent toutefois à cet égard. En premier lieu, les données médico-administratives du SNIIRAM-SNDS sont complexes, et les chercheurs ne les connaissent pas nécessairement. Pour déterminer quelle extraction de données issues du SNDS est requise par le projet déposé par un chercheur, de nombreux allers-retours sont souvent nécessaires entre le chercheur et les responsables de données travaillant à la CNAM. Soit, par exemple, un chercheur souhaitant enquêter sur la cohorte des diabétiques en 2018 : il existe en réalité plusieurs types de diabétiques, répondant dans le SNDS à différentes définitions. Ainsi, le chercheur devra notamment préciser si les patients qui l'intéressent sont fortement traités (donc sous insuline), ou s'ils reçoivent trois, ou six, traitements antidiabétiques par trimestre, ce qui renvoie chaque fois à des catégories différentes. Le chercheur devra ainsi définir la notion de « diabétique » qui l'intéresse à travers des données administratives, et non médicales : il ne suffira pas de demander l'ensemble des personnes présentant tel ou tel niveau de glycémie lors de leurs tests. Il n'est donc pas simple de passer de l'idée d'un projet à la caractérisation des données à exploiter. Ce point a toujours été sous-estimé par les chercheurs. Bien sûr, nous travaillons avec le HDH pour délivrer une formation à tout chercheur qui dépose un projet, pour lui expliquer comment sont constituées les données, ce qu'il est possible d'en tirer et la manière de les traiter. Elles font également l'objet d'une documentation publique et ouverte à tous, de plus en plus volumineuse. La nécessité d'obtenir l'autorisation de la CNIL ne constitue donc pas nécessairement le principal problème dans la complexité actuelle du processus d'accès aux données.

Par ailleurs, les projets déposés sont nombreux, ce qui constitue une charge importante pour le CESREES comme pour la CNIL. Des travaux sont donc en cours entre la CNIL, le Health Data Hub et le ministère, pour encadrer le principe général des études susceptibles d'être autorisées, et les méthodologies de référence dans lesquelles elles pourront s'inscrire pour accéder plus rapidement aux données. Un échange restera néanmoins nécessaire au terme de ce parcours pour déterminer quelles données le chercheur souhaite exactement extraire du SNDS. Les travaux de fluidification en cours sont donc nécessaires, et ils pourraient simplifier les parcours d'accès aux données pour un certain nombre d'études, mais il faut bien comprendre que ces données ne sont pas nativement construites pour la recherche, et qu'elles nécessitent un travail d'appropriation, généralement complexe, par les chercheurs. Naturellement, de plus en plus d'unités de recherche et de cabinets d'étude ont cependant déjà eu accès aux données du SNDS, et savent donc exprimer leurs besoins de manière pertinente et efficace. Tous les chercheurs « naïfs SNDS » (pour reprendre une expression courante en

médecine) ont quant à eux besoin d'un certain temps pour comprendre quelles données sont présentes dans le SNDS et pouvoir les utiliser.

Or, comme vous le savez sans doute, et comme cela a dû être signalé par de nombreuses personnes au cours de vos auditions, le milieu de la recherche est en réalité très concurrentiel, et assez peu coopératif. Les producteurs d'une cohorte souhaitent donc d'abord valoriser leurs propres travaux sur cette cohorte avant de laisser les autres l'exploiter. Un vrai accompagnement des producteurs de données est donc nécessaire, pour qu'ils passent d'une attitude de propriétaire, à une volonté de partage de l'ensemble de leurs données. L'un des rôles du Health Data Hub est ainsi de réunir les « propriétaires » ou producteurs de données pour définir avec eux les conditions d'un partage qui reconnaisse aussi la tâche de production des données et la nécessité d'un retour sur investissement pour ceux qui s'attachent à produire des données, qui sont parfois exploitées par d'autres. Ce retour sur investissement est naturellement extrêmement important pour que les chercheurs continuent à construire des données et à les partager.

De la loi de 2019, résultent le SNDS élargi et un cadre réglementaire pour faciliter les appariements. Le HDH a aussi repris les missions de l'INDS pour les étendre à l'accompagnement de projets, au partage et à l'amélioration de l'usage des données pour l'ensemble des porteurs. Cette mission de fédération des acteurs est extrêmement importante pour le HDH.

S'agissant du choix de Microsoft par le Health Data Hub pour héberger ses données, je laisserai Mme Stéphanie Naux s'exprimer dans un premier temps.

Mme Stéphanie Naux. Lorsque vous avez reçu la directrice du Health-Data Hub, elle vous a expliqué les raisons de ses choix opérationnels. Il nous semble essentiel de trouver un équilibre entre, d'une part, la nécessité (totalement reconnue par la CNAM) de pouvoir utiliser plus largement et plus rapidement les données, dans l'intérêt de la santé de la population et de la recherche, et, d'autre part, les impératifs de sécurité des données (que la CNAM garantit depuis longtemps) et de maîtrise des usages. Cette maîtrise constitue en effet une priorité de très haut niveau pour la CNAM, en tant que responsable du traitement du SNDS et de la constitution de la base principale.

Lorsque la CNAM a construit le SNIIRAM et établi ses propres choix d'organisation à cette fin, la question du *cloud* ne se posait pas. Dès lors qu'elle a retenu le principe d'une architecture propriétaire, elle n'a pas été conduite à s'interroger, comme le Health Data Hub, sur la question du *cloud*, d'autant plus qu'il paraissait naturel de conserver cette architecture pour des données issues très largement des processus de gestion interne de l'assurance maladie.

M. Claude Gissot. Le conseil de la CNAM a ensuite été saisi par le ministère pour rendre un avis sur le décret dit « SNDS » (qui vise à organiser l'application de la loi de 2019), et, bien que cela ne fasse pas l'objet du décret, il a cherché à apprécier l'ensemble des conditions du projet HDH, et notamment les conditions d'hébergement de la plateforme. Compte tenu de la décision du Conseil d'État et de l'engagement du ministre sur le futur hébergement, cette question de l'hébergement doit être traitée le plus rapidement possible. Toutefois, comme cela a été signalé, la question du *cloud* souverain ne porte pas seulement sur les données de santé, même si celles-ci, de par leur sensibilité, et particulièrement celles du HDH, peuvent naturellement figurer parmi les premières concernées.

Le conseil de la CNAM a donc estimé nécessaire de trouver une solution à court terme à ce problème, et exprimé son opposition au transfert de la base de données centrale avant que

cette solution soit trouvée. Son communiqué a néanmoins rappelé également qu'une plus grande utilisation des données était indispensable pour la médecine et la santé des assurés.

Par ailleurs, la CNIL a malgré tout autorisé la poursuite de projets sur la plateforme du HDH, s'agissant notamment de projets liés à la crise du Covid-19.

Il convient cependant de rappeler que le cadre fixé pour la transmission de ces données relève du pouvoir législatif et réglementaire sous le contrôle de la CNIL. Plusieurs étapes doivent encore être franchies avant d'en arriver là : la parution du décret SNDS, et la demande à la CNIL par la plateforme HDH, d'une autorisation pour traiter l'ensemble du SNDS. Mais, dès lors qu'un cadre juridique aura été fixé par ces textes et par ces autorités, la CNAM l'appliquera.

Mme Stéphanie Naux. La sécurité du SNDS fait l'objet d'un dispositif d'amélioration continue, qui date du SNIIRAM et qui a été contrôlé par la CNIL. Il ne s'agit pas d'un sujet récent pour la CNAM, même si l'actualité en rappelle souvent le caractère essentiel. Pour la CNAM, son enjeu dépasse également le seul SNDS, puisqu'elle gère des données de santé selon un périmètre plus large, et que des démarches de sécurité les concernent toutes.

S'agissant spécifiquement du SNDS, sa sécurité est encadrée par différents référentiels, dont un qui lui est spécifique, et qui est porté par un arrêté dédié, avec un niveau d'exigence de sécurité élevé. Il comprend un certain nombre de mesures spécifiques, comprenant un système d'authentification forte pour l'accès aux données et une vérification importante de la minimisation et du périmètre d'accès aux données personnelles, afin de s'assurer que les personnes autorisées accèdent uniquement aux données conformes aux autorisations délivrées par la CNIL. Tout ce processus s'inscrit dans des garanties contractuelles importantes. Les personnes physiques accédant aux données sont identifiées sous l'autorité du responsable de l'institution dont elles dépendent, qu'il s'agisse des accès permanents ou des accès sur projet. Les exportations de données non strictement anonymes sont interdites. Bien que pseudonymisées, les données du SNDS ne peuvent ainsi être utilisées et étudiées que dans des univers conformes au référentiel de sécurité. Seules peuvent être exportées des données strictement anonymes, donc fortement agrégées, la doctrine de la CNIL étant assez stricte en matière d'anonymat. Un système de traçabilité de l'activité des utilisateurs, et tout un ensemble de mesures techniques et organisationnelles faisant l'objet de revues régulières et de plans d'action ont été mis en place pour assurer cette sécurité de manière continue. Tout ce système de la CNAM est homologué, comme toutes les autres bulles susceptibles de recevoir des données du SNDS, ce qui permet de réajuster les risques à prendre en compte, et de mettre en place les mesures correctives requises pour les éliminer ou les diminuer.

M. Philippe Latombe, rapporteur. Depuis deux jours, une consultation a été lancée par la CNIL à propos des entrepôts de données de santé, afin d'aboutir à un cadre harmonisé entre tous ces entrepôts et à une doctrine en France plus cohérente. Constatez-vous aujourd'hui une distorsion entre les données de santé recueillies à différents endroits du territoire, lorsqu'il est ensuite demandé de les corréler ou de les mettre en cohorte avec des données du SNDS ? Les pratiques, les modes de fonctionnement et l'attachement aux données de santé varient-ils en fonction des territoires ?

M. Claude Gissot. Je ne suis pas en mesure de vous répondre. Parmi les données de santé, il faut distinguer, en premier lieu, les données individuelles nominatives destinées à la gestion, et qu'on trouve dans les établissements de santé, etc. : pour ces données aussi, des questions de sécurité se posent, mais chacun de ces systèmes d'information se déclare à la CNIL, en précisant ses conditions de sécurité, et il revient à la CNIL d'autoriser ou non le traitement de ces données. En deuxième lieu, il existe des données pseudonymisées telles que

nous vous les avons présentées, et qu'on trouve également dans des entrepôts hospitaliers, comme celui de l'AP-HP, même si elles n'utilisent pas nécessairement le même pseudonyme, et ne sont donc pas interconnectables immédiatement. Pour ces entrepôts aussi, une autorisation de la CNIL est nécessaire, sur la base d'une description du traitement et de l'ensemble des sécurités prévus pour ces données.

La CNIL a donc tout intérêt à mettre ces systèmes en cohérence, à défaut de les uniformiser, car chacun d'eux présente ses propres spécificités.

M. Philippe Latombe, rapporteur. Parler d'une mise en cohérence semble en effet adéquat.

M. Claude Gissot. Il s'agit de mettre ces systèmes en cohérence et de supprimer les écarts évoqués, s'ils existent, mais je ne dispose d'aucune documentation sur ces écarts. Je ne connais pas tous les systèmes d'information.

Mme Stéphanie Naux. Ces dernières années, la CNIL a été plusieurs fois sollicitée pour autoriser la mise en place d'entrepôts par différents acteurs, mais elle manquait souvent de bases juridiques à cette fin. Les dispositions de la loi Informatique et libertés ne lui laissaient pas nécessairement la latitude d'autoriser des entrepôts. Elle avait la possibilité d'autoriser des traitements, assortis de finalités, mais il lui était plus difficile juridiquement d'autoriser un réservoir de données susceptible de différentes utilisations. Des évolutions du texte ont eu lieu en ce sens, et il s'agit maintenant d'harmoniser les contraintes juridiques diversifiées dans lesquelles les entrepôts ont dû se constituer.

M. Philippe Latombe, rapporteur. Nombre des intervenants que nous avons auditionnés à propos des données de santé ont évoqué la question de leur valorisation. En quoi consisterait selon vous la valorisation des données du SNDS ?

M. Claude Gissot. Dans certains pays, les données s'échangent monétairement.

M. Philippe Latombe, rapporteur. Ce n'est pas le cas chez nous.

M. Claude Gissot. Ce n'est pas le cas chez nous, où les données administratives, notamment, ne sont finalement que réutilisées, puisqu'elles sont collectées pour nos propres usages de gestion, de sorte que la collecte est déjà assumée dans nos missions de remboursement de soins, etc. Je ne sais pas si vous avez interrogé la direction de la recherche, des études, de l'évaluation et des statistiques (DREES) ou le ministère sur cette question, mais aujourd'hui, la donnée SNDS n'est pas valorisable.

La question des services créés autour de la donnée peut toutefois se poser, car leurs utilisateurs peuvent être amenés à rémunérer les services créés par exemple par un groupement hospitalier (GH). Toutefois, l'objectif de ces services est plutôt de faciliter l'usage des données, et de les rendre les plus accessibles possible. Aucune valorisation de la donnée elle-même n'existe donc en soi.

La valorisation pour les producteurs se conçoit plutôt en termes de rôle ou d'image. Pour certains instituts de recherche, elle peut consister à gagner des points dans le système d'interrogation, de gestion, d'analyse des publications scientifiques (SIGAPS), permettant de valoriser l'activité de recherche. L'activité de constitution de bases de données par la recherche constituerait évidemment une forme de valorisation, au même titre que le fait d'être nommé dans les articles utilisant ces données, puisque ce type de références sont très importantes pour la recherche.

Les données de santé du SNDS ou du HDH sont de toute manière d'intérêt public. Or, l'intérêt public ne se monnaye pas. Leur valorisation vient du fait qu'elles sont partagées dans la collectivité, qu'elles servent à réaliser de bonnes études et à améliorer la prise en charge et la santé des patients.

M. Philippe Latombe, rapporteur. Les systèmes de santé sont différents entre tous les pays, mais des données de santé sont quand même collectées dans nos pays voisins. Échangez-vous avec vos « homologues » européens ? Examinez-vous leurs pratiques et certains de leurs modes de fonctionnement mériteraient-ils d'être importés ? À l'inverse, certaines de leurs pratiques doivent-elles absolument être évitées ?

M. Claude Gissot. Nous suivons en effet nos pratiques respectives de manière rapprochée. Même si nos échanges ne visent pas nécessairement à harmoniser les pratiques entre tous les pays, plusieurs initiatives européennes sont en cours pour mettre en place un espace européen des données de santé et faciliter l'utilisation des données de santé dans le cadre européen.

Les autres systèmes de santé ont souvent été créés de manière différente, mais aussi avec des pratiques de gestion des données assez différentes. Il est courant d'opposer les pays du Nord et du Sud : ils s'opposent sur ce point également. La pratique de la connexion des fichiers est ainsi souvent plus répandue dans les pays du Nord que dans les pays du Sud comme la France. L'appariement et l'utilisation croisée des sources sont beaucoup plus facilement acceptés dans les pays du Nord (le Danemark, la Suède, etc.). Ce n'est pas seulement une question de droit : la manière de gérer les données et l'acceptation du partage des données, même fines, sont aussi des faits de société.

En Angleterre, la *Clinical Practice Research Database (CPRD)* est intéressante, dans la mesure précisément où elle combine des données médicales et des données médico-administratives, mais elle ne l'a pas fait de manière exhaustive jusqu'à présent, ce qui lui confère une moindre puissance statistique.

Aux États-Unis, les données sont beaucoup plus riches, mais elles sont encore plus « silotées » qu'ici, puisqu'elles sont collectées par assureur. Même *Medicare* et *Medicaid* ne permettent donc pas de disposer d'une vision d'ensemble du système de santé, puisque toute une partie de la population n'y sera pas prise en compte.

En Allemagne, les systèmes d'assurance sont régionalisés également, même s'il existe certainement des bases de données communes. En Espagne et en Italie aussi, la collecte est relativement régionalisée.

Ce qui nous intéresse est d'examiner de quelles pratiques nous pourrions nous inspirer. Le HDH porte également cette démarche. La base de données médico-administratives centrale SNDS-SNIIRAM-PMSI est très utile, très utilisée et totalement exhaustive, avec une puissance statistique sans égal, mais il y manque un certain nombre d'informations médicales, ou médicalisées, qui constitueraient le complément idéal pour favoriser les études, les recherches, et finalement les innovations en santé. Nous pourrions nous inspirer d'autres pays à ce sujet, mais nous sommes parfaitement conscients de cet écart.

M. Philippe Latombe, rapporteur. Les citoyens français sont-ils aujourd'hui très attachés à leurs données de santé ? Leur accordent-ils une plus grande importance qu'auparavant, et sont-ils plus vigilants ? Constatez-vous un changement d'état d'esprit de nos concitoyens vis-à-vis des données de santé ? De ce point de vue, le compte AMELI a-t-il été reçu en tant que marque bénéficiant de la confiance des citoyens quant à la protection des données de santé qu'elle apporte ?

M. Claude Gissot. L'assurance maladie d'une manière générale est reconnue par ses assurés comme gérant leurs données de santé avec beaucoup d'attention et de précautions. Même si les enquêtes que nous réalisons ne portent que sur la perception qu'ont nos assurés de nos actions, elles font en tout cas ressortir que nos assurés nous font confiance,

Il faut toutefois développer la compréhension des données de santé et de leurs usages par le citoyen. Je ne sais pas si une évolution peut être mesurée à cet égard, car nous ne disposons pas d'un point zéro, ou d'une mesure de l'état de cette compréhension, il y a dix ans. Les débats afférents sont de plus en plus actifs dans la presse et dans la sphère publique ouverte. Il existe un réel besoin, pour les citoyens, de parvenir à maîtriser les données de santé et leurs usages, ce qui n'est évidemment pas le cas aujourd'hui. Lorsque nous offrons des services, que ce soit le compte AMELI ou le DMP, nous essayons d'être les plus clairs possible concernant l'usage qui y est fait des données. S'agissant du SNDS, la situation est différente, puisque les données sont pseudonymisées et ne donnent pas lieu à des usages individuels, mais collectifs de santé publique. Le degré de connaissance de ces enjeux est certainement encore très hétérogène selon les citoyens, et il faut d'ailleurs en reconnaître la complexité. Notre discussion et les auditions que vous conduisez aujourd'hui en attestent.

Il est important en tout cas que les associations de patients, et France Assos Santé en particulier, soient bien représentées dans le Health Data Hub, comme au conseil de la CNAM, etc., car elles constituent le bon intermédiaire avec les patients isolés, qui ne savent pas nécessairement quoi faire de leurs données de santé, ou ne voient pas l'intérêt de les partager. Elles constituent donc un vecteur très important pour faire progresser la conscience de ces enjeux.

Mme Stéphanie Naux. L'un des indicateurs les plus factuels dont nous disposions à cet égard tient aux remontées d'exercice de leurs droits par les personnes ou au nombre de questions qu'elles posent à ce sujet. Or, nous n'avons pas observé d'évolution majeure de ce point de vue.